

INVARIANTS OF $GL_n(\mathbb{F}_q)$ IN POLYNOMIALS MOD FROBENIUS POWERS

J. LEWIS, V. REINER, AND D. STANTON

ABSTRACT. Conjectures are given for Hilbert series related to polynomial invariants of finite general linear groups, one for invariants mod Frobenius powers of the irrelevant ideal, one for cofixed spaces of polynomials.

1. INTRODUCTION

This paper proposes two related conjectures in the invariant theory of $GL_n(\mathbb{F}_q)$, motivated by the following celebrated result of L.E. Dickson [7]; see also [5, Thm. 8.1.1], [23, Thm. 8.1.5].

Theorem. *When $G := GL_n(\mathbb{F}_q)$ acts via invertible linear substitutions of variables on the polynomial algebra $S = \mathbb{F}_q[x_1, \dots, x_n]$, the G -invariants form a polynomial subalgebra $S^G = \mathbb{F}_q[D_{n,0}, D_{n,1}, \dots, D_{n,n-1}]$.*

Here the *Dickson polynomials* $D_{n,i}$ are the coefficients in the expansion $\prod_{\ell(\mathbf{x})} (t + \ell(\mathbf{x})) = \sum_{i=0}^n D_{n,i} t^{q^i}$ where the product runs over all \mathbb{F}_q -linear forms $\ell(\mathbf{x})$ in the variables x_1, \dots, x_n . In particular, $D_{n,i}$ is homogeneous of degree $q^n - q^i$, so that Dickson's Theorem implies this *Hilbert series* formula:

$$(1.1) \quad \text{Hilb}(S^G, t) := \sum_{d \geq 0} \dim_{\mathbb{F}_q}(S^G)_d t^d = \prod_{i=0}^{n-1} \frac{1}{1 - t^{q^n - q^i}}.$$

Our main conjecture gives the Hilbert series for the G -invariants in the quotient ring $Q := S/\mathfrak{m}^{[q^m]}$ by an iterated *Frobenius power* $\mathfrak{m}^{[q^m]} := (x_1^{q^m}, \dots, x_n^{q^m})$ of the *irrelevant ideal* $\mathfrak{m} = (x_1, \dots, x_n)$. The ideal $\mathfrak{m}^{[q^m]}$ is G -stable, and hence the G -action on S descends to an action on the quotient Q .

Conjecture 1.1. *The G -fixed subalgebra Q^G has Hilbert series $\text{Hilb}((S/\mathfrak{m}^{[q^m]})^G, t) = C_{n,m}(t)$ where*

$$(1.2) \quad C_{n,m}(t) := \sum_{k=0}^{\min(n,m)} t^{(n-k)(q^m - q^k)} \begin{bmatrix} m \\ k \end{bmatrix}_{q,t}.$$

The (q, t) -*binomial* appearing in (1.2) is a polynomial in t , introduced and studied in [18], defined by

$$(1.3) \quad \begin{bmatrix} n \\ k \end{bmatrix}_{q,t} := \frac{\text{Hilb}(S^{P_k}, t)}{\text{Hilb}(S^G, t)} = \prod_{i=0}^{k-1} \frac{1 - t^{q^n - q^i}}{1 - t^{q^k - q^i}}.$$

Here P_k is a *maximal parabolic subgroup* of G stabilizing $\mathbb{F}_q^k \subset \mathbb{F}_q^n$, so G/P_k is the *Grassmannian* of k -planes.

It will be shown in Section 3 that Conjecture 1.1 implies the following conjecture on the G -cofixed space (also known as the *maximal G -invariant quotient* or the *G -coinvariant space*¹) of S . This is defined to be the quotient \mathbb{F}_q -vector space $S_G := S/N$ where N is the \mathbb{F}_q -linear span of all polynomials $g(f) - f$ with f in S and g in G .

Conjecture 1.2. *The G -cofixed space of $S = \mathbb{F}_q[x_1, \dots, x_n]$ has Hilbert series*

$$\text{Hilb}(S_G, t) = \sum_{k=0}^n t^{n(q^k - 1)} \prod_{i=0}^{k-1} \frac{1}{1 - t^{q^k - q^i}}.$$

(Here and elsewhere we interpret empty products as 1, as in the $k = 0$ summand above.)

Date: March 27, 2014.

Key words and phrases. finite general linear group, Frobenius power, Dickson invariants, cofixed, fixed quotient, coinvariant, divided power invariants, reflection group, Catalan, parking, cyclic sieving.

Work partially supported by NSF grants DMS-1148634 and DMS-1001933.

¹Warning: this last terminology is often used for a *different* object, the quotient ring $S/(D_{n,0}, \dots, D_{n,n-1})$, so we avoid it.

Example 1.3. When $n = 0$, Conjectures 1.1 and 1.2 have little to say, since $S = \mathbb{F}_q$ has no variables and $G = GL_0(\mathbb{F}_q)$ is the trivial group. When $n = 1$, both conjectures are easily verified as follows. The group $G = GL_1(\mathbb{F}_q) = \mathbb{F}_q^\times$ is cyclic of order $q - 1$. A cyclic generator g for G scales the monomials in $S = \mathbb{F}_q[x]$ via $g(x^k) = (\zeta x)^k = \zeta^k x^k$ where ζ is a $(q - 1)$ st root of unity in \mathbb{F}_q ; g similarly scales the monomial basis elements $\{1, \bar{x}, \bar{x}^2, \dots, \bar{x}^{q^m-1}\}$ of the quotient ring $Q = S/\mathfrak{m}^{[q^m]}$. Hence \bar{x}^k is G -invariant in Q if and only if $q - 1$ divides k , so that Q^G has \mathbb{F}_q -basis $\{1, \bar{x}^{q-1}, \bar{x}^{2(q-1)}, \dots, \bar{x}^{q^m-q}, \bar{x}^{q^m-1}\}$. Therefore

$$\text{Hilb}(Q^G, t) = (1 + t^{q-1} + t^{2(q-1)} + \dots + t^{q^m-q}) + t^{q^m-1} = t^0 \begin{bmatrix} m \\ 1 \end{bmatrix}_{q,t} + t^{q^m-1} \begin{bmatrix} m \\ 0 \end{bmatrix}_{q,t} = C_{1,m}(t).$$

For the same reason, the image of x^k survives as an \mathbb{F}_q -basis element in the G -cofixed quotient S_G if and only if $q - 1$ divides k . Hence S_G has \mathbb{F}_q -basis given by the images of $\{1, x^{q-1}, x^{2(q-1)}, \dots\}$, so that

$$\text{Hilb}(S_G, t) = 1 + t^{q-1} + t^{2(q-1)} + \dots = \frac{1}{1 - t^{q-1}} = 1 + \frac{t^{q-1}}{1 - t^{q-1}}.$$

1.1. The parabolic generalization. In fact, we will work with generalizations of Conjectures 1.1 and 1.2 to a *parabolic subgroup* P_α of G specified by a *composition* $\alpha = (\alpha_1, \dots, \alpha_\ell)$ of n , so that $|\alpha| := \alpha_1 + \dots + \alpha_\ell = n$, and $\alpha_i > 0$ without loss of generality. This P_α is the subgroup of block upper-triangular invertible matrices

$$g = \begin{bmatrix} g_1 & * & \cdots & * \\ 0 & g_2 & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & g_\ell \end{bmatrix}$$

with diagonal blocks g_1, \dots, g_ℓ of sizes $\alpha_1 \times \alpha_1, \dots, \alpha_\ell \times \alpha_\ell$. A generalization of Dickson's Theorem proven by Mui [17] and Hewett [11] asserts that S^{P_α} is again a polynomial algebra, having Hilbert series given by the following expression, where we denote partial sums of α by $A_i := \alpha_1 + \dots + \alpha_i$:

$$(1.4) \quad \text{Hilb}(S^{P_\alpha}, t) = \prod_{i=1}^{\ell} \prod_{j=0}^{\alpha_i-1} \frac{1}{1 - t^{q^{A_i} - q^{A_{i-1}+j}}}.$$

This leads to a polynomial in t called the (q, t) -*multinomial*, also studied in [18]:

$$(1.5) \quad \left[\begin{matrix} n \\ \alpha \end{matrix} \right]_{q,t} := \frac{\text{Hilb}(S^{P_\alpha}, t)}{\text{Hilb}(S^G, t)} = \frac{\prod_{j=0}^{n-1} (1 - t^{q^n - q^j})}{\prod_{i=1}^{\ell} \prod_{j=0}^{\alpha_i-1} (1 - t^{q^{A_i} - q^{A_{i-1}+j}})}.$$

To state the parabolic versions of the conjectures, we consider *weak compositions* $\beta = (\beta_1, \dots, \beta_\ell)$ with $\beta_i \in \mathbb{Z}_{\geq 0}$, of a fixed length ℓ , and partially order them *componentwise*, that is, $\beta \leq \alpha$ if $\beta_i \leq \alpha_i$ for $i = 1, 2, \dots, \ell$. In this situation, let $B_i := \beta_1 + \beta_2 + \dots + \beta_i$.

Parabolic Conjecture 1.1. For $m \geq 0$ and for α a composition of n , the P_α -fixed subalgebra Q^{P_α} of the quotient ring $Q = S/\mathfrak{m}^{[q^m]}$ has Hilbert series $\text{Hilb}(Q^{P_\alpha}, t) = C_{\alpha,m}(t)$, where

$$(1.6) \quad C_{\alpha,m}(t) := \sum_{\substack{\beta: \beta \leq \alpha \\ |\beta| \leq m}} t^{e(m, \alpha, \beta)} \left[\begin{matrix} m \\ \beta, m - |\beta| \end{matrix} \right]_{q,t} \quad \text{with} \quad e(m, \alpha, \beta) := \sum_{i=1}^{\ell} (\alpha_i - \beta_i)(q^m - q^{B_i}).$$

The $\ell = 1$ case of Parabolic Conjecture 1.1 is Conjecture 1.1. Parabolic Conjecture 1.1 also implies the following conjecture.

Parabolic Conjecture 1.2. For a composition α of n , the P_α -cofixed space S_{P_α} of S has Hilbert series

$$(1.7) \quad \text{Hilb}(S_{P_\alpha}, t) = \sum_{\beta: \beta \leq \alpha} t^{\sum_{i=1}^{\ell} \alpha_i (q^{B_i} - 1)} \prod_{i=1}^{\ell} \prod_{j=0}^{\beta_i-1} \frac{1}{1 - t^{q^{B_i} - q^{B_{i-1}+j}}}.$$

Similarly, the $\ell = 1$ case of Parabolic Conjecture 1.2 is Conjecture 1.2.

1.2. Structure of the paper. The rest of the paper explains the relation between Parabolic Conjectures 1.1 and 1.2, along with context and evidence for both, including relations to known results.

Section 2 explains why Parabolic Conjecture 1.1 implies the Hilbert series (1.4) in the limit as $m \rightarrow \infty$, with proof delayed until Appendix A.

Section 3 shows that Parabolic Conjecture 1.1 implies Parabolic Conjecture 1.2. It then shows the reverse implication in the case $n = 2$. Appendix B proves both via direct arguments for $n = 2$.

Section 4 checks Parabolic Conjecture 1.1 for $m = 0, 1$.

Section 5 explains why the P_α -cofixed space S_{P_α} is a finitely generated module of rank one over the P_α -fixed algebra S^{P_α} , and why this is consistent with the form of Parabolic Conjecture 1.2.

Section 6 concerns some of our original combinatorial motivation, comparing two G -representations:

- on the graded quotient $Q = S/\mathfrak{m}^{[q^m]}$, versus
- permuting the points of $(\mathbb{F}_{q^m})^n$.

These two representations are *not* isomorphic; however, we will show that they have the same composition factors, that is, they are *Brauer-isomorphic*. After extending scalars from $\mathbb{F}_q G$ to $\mathbb{F}_{q^m} G$ -modules, this Brauer-isomorphism holds even taking into account a commuting group action $G \times C$, where the cyclic group $C = \mathbb{F}_{q^m}^\times$ is the multiplicative group of \mathbb{F}_{q^m} . Consistent with this, Parabolic Conjecture 1.1 has a strange implication: the two representations have G -fixed spaces and P_α -fixed spaces which are *isomorphic* C -representations. This assertion is equivalent to the fact that evaluating $C_{\alpha,m}(t)$ when t is a $(q^m - 1)$ st root of unity exhibits a *cyclic sieving phenomenon* in the sense of [19].

Section 7 collects some further questions and remarks.

ACKNOWLEDGEMENTS

The authors thank A. Broer, M. Crabb, A. Shepler, L. Smith, and P. Webb for valuable suggestions and references, as well as D. Stamate for computations discussed in Example 5.12 supporting Conjecture 5.9.

2. CONJECTURE 1.1 IMPLIES (1.4)

The following proposition is delicate to verify, but serves two purposes, explained after its statement.

Proposition 2.1. *For any $m \geq 0$ and any composition α of n , the power series*

$$\text{Hilb}(S^{P_\alpha}, t) = \prod_{i=1}^{\ell} \prod_{j=0}^{\alpha_i-1} \frac{1}{1 - t^{q^{A_i} - q^{A_{i-1} + j}}}$$

is congruent in $\mathbb{Z}[[t]]/(t^{q^m})$ to the polynomial

$$C_{\alpha,m}(t) = \sum_{\substack{\beta: \beta \leq \alpha \\ |\beta| \leq m}} t^{e(m, \alpha, \beta)} \left[\begin{matrix} m \\ \beta, m - |\beta| \end{matrix} \right]_{q,t} \quad \text{where} \quad e(m, \alpha, \beta) = \sum_{i=1}^{\ell} (\alpha_i - \beta_i)(q^m - q^{B_i}).$$

The first purpose of Proposition 2.1 is to give evidence for Parabolic Conjecture 1.1, since it is implied by the conjecture: the ideal $\mathfrak{m}^{[q^m]} = (x_1^{q^m}, \dots, x_n^{q^m})$ only contains elements of degree q^m and above, so the G -equivariant quotient map $S \twoheadrightarrow Q = S/\mathfrak{m}^{[q^m]}$ restricts to \mathbb{F}_q -vector space isomorphisms

$$(2.1) \quad \begin{aligned} S_d &\cong Q_d \\ S_d^{P_\alpha} &\cong Q_d^{P_\alpha} \end{aligned}$$

for $0 \leq d \leq q^m - 1$. Consequently one has

$$(2.2) \quad \text{Hilb}(S^{P_\alpha}, t) \equiv \text{Hilb}(Q^{P_\alpha}, t) \pmod{(t^{q^m})}.$$

In particular, Proposition 2.1 shows why Parabolic Conjecture 1.1 gives (1.4) in the limit as $m \rightarrow \infty$.

Secondly, the precise form of Proposition 2.1 will be used in the proof of Corollary 3.6, asserting the equivalence of Parabolic Conjectures 1.1 and 1.2 for $n = 2$.

The proof of Proposition 2.1 is rather technical, so it is delayed until Appendix A.

3. CONJECTURE 1.1 IMPLIES CONJECTURE 1.2

The desired implication will come from an examination of the quotient ring

$$Q := S/\mathfrak{m}^{[q^m]} = \mathbb{F}_q[x_1, \dots, x_n]/(x_1^{q^m}, \dots, x_n^{q^m})$$

as a *monomial complete intersection*, and hence a *Gorenstein ring*. Note that Q has monomial basis

$$(3.1) \quad \{\mathbf{x}^a := x_1^{a_1} \cdots x_n^{a_n}\}_{0 \leq a_i \leq q^m - 1}$$

and that its homogeneous component Q_{d_0} of top degree

$$(3.2) \quad d_0 := n(q^m - 1)$$

is 1-dimensional, spanned over \mathbb{F}_q by the image of the monomial

$$\mathbf{x}^{a_0} := (x_1 \cdots x_n)^{q^m - 1}.$$

Furthermore, the \mathbb{F}_q -bilinear pairing

$$(3.3) \quad \begin{aligned} Q_i \otimes Q_j &\longrightarrow Q_{d_0} = \mathbb{F}_q \cdot \mathbf{x}^{a_0} \cong \mathbb{F}_q \\ (f_1, f_2) &\longmapsto f_1 \cdot f_2 \end{aligned}$$

is *non-degenerate* (or *perfect*): for monomials $\mathbf{x}^a, \mathbf{x}^b$ in (3.1) of degrees i, j with $i + j = d_0$, one has

$$(\mathbf{x}^a, \mathbf{x}^b) = \begin{cases} \mathbf{x}^{a_0} & \text{if } a + b = a_0, \\ 0 & \text{otherwise.} \end{cases}$$

Proposition 3.1. *The monomial $\mathbf{x}^{a_0} = (x_1 \cdots x_n)^{q^m - 1}$ has G -invariant image in the quotient $Q = S/\mathfrak{m}^{[q^m]}$, and hence its span Q_{d_0} carries the trivial G -representation.*

Proof 1. As G acts on S and on Q preserving degree, it induces a 1-dimensional G -representation on Q_{d_0} . Thus Q_{d_0} must carry one of the linear characters of $G = GL_n(\mathbb{F}_q)$, that is, \det^j for some j in $\{0, 1, \dots, q-2\}$. We claim that in fact $j = 0$, since the element g in G that scales the variable x_1 by a primitive $(q-1)$ st root of unity γ in \mathbb{F}_q^\times and fixes all other variables x_i with $i \geq 2$ will have $\det(g) = \gamma$ and has $g(\mathbf{x}^{a_0}) = \gamma^{q^m - 1} \mathbf{x}^{a_0} = \mathbf{x}^{a_0}$. \square

Proof 2. Note $G = GL_n(\mathbb{F}_q)$ is generated by all *permutations* of coordinates, all *scalings* of coordinates, and any *transvection*, such as the element u sending $x_1 \mapsto x_1 + x_2$ and fixing x_i for $i \neq 1$. So it suffices to check that the image of $\mathbf{x}^{a_0} = (x_1 \cdots x_n)^{q^m - 1}$ in Q is invariant under permutations (obvious), invariant under scalings of a coordinate (easily checked as in Proof 1), and invariant under the transvection u :

$$u(\mathbf{x}^{a_0}) = (x_1 + x_2)^{q^m - 1} (x_2 \cdots x_n)^{q^m - 1} = (x_1^{q^m - 1} + x_2 h)(x_2 \cdots x_n)^{q^m - 1} \equiv \mathbf{x}^{a_0} \pmod{\mathfrak{m}^{[q^m]}},$$

where h is a polynomial whose exact form is unimportant. \square

Note that Proposition 3.1 is an expected consequence of Conjecture 1.1, due to the following observation.

Proposition 3.2. *For any composition α of n , the polynomial $C_{\alpha, m}(t)$ is monic of degree $d_0 = n(q^m - 1)$.*

Proof. Letting $\deg_t(-)$ denote degree in t , the product formula (1.5) for the (q, t) -multinomial shows that

$$(3.4) \quad \begin{aligned} \deg_t \left[\begin{matrix} m \\ \beta, m - |\beta| \end{matrix} \right]_{q, t} &= \sum_{j=0}^{|\beta|} (q^m - q^j) - \sum_{i=1}^{\ell} \sum_{j=0}^{\beta_i - 1} (q^{B_i} - q^{B_{i-1} + j}) \\ &= |\beta| q^m - \sum_{j=0}^{|\beta|} q^j - \sum_{i=1}^{\ell} \beta_i q^{B_i} + \sum_{i=1}^{\ell} \sum_{j=0}^{\beta_i - 1} q^{B_{i-1} + j} \\ &= |\beta| q^m - \sum_{i=1}^{\ell} \beta_i q^{B_i}, \end{aligned}$$

while the exponent on the monomial $t^{e(m, \alpha, \beta)}$ can be rewritten

$$(3.5) \quad e(m, \alpha, \beta) = \sum_{i=1}^{\ell} (\alpha_i - \beta_i) (q^m - q^{B_i}) = nq^m - |\beta| q^m - \sum_{i=1}^{\ell} \alpha_i q^{B_i} + \sum_{i=1}^{\ell} \beta_i q^{B_i}.$$

Therefore the summand of $C_{\alpha,m}(t)$ indexed by β has degree equal to the sum of (3.4) and (3.5), namely

$$nq^m - \sum_{i=1}^{\ell} \alpha_i q^{B_i} \geq nq^m - \sum_{i=1}^{\ell} \alpha_i = nq^m - n = n(q^m - 1) = d_0.$$

Equality occurs in this inequality if and only $B_i = 0$ for all i , so the t -degree is maximized uniquely by the $\beta = 0$ summand, which is the single monomial $t^{n(q^m-1)} = t^{d_0}$. \square

Proposition 3.1 shows that the nondegenerate pairing (3.3) is G -invariant: for any g in G , one has

$$(g(f_1), g(f_2)) = g(f_1)g(f_2) = g(f_1 f_2) = f_1 f_2 = (f_1, f_2).$$

Thus one has an isomorphism of G -representations $Q_i \cong Q_j^*$ in complementary degrees $i + j = d_0$. Here the notation U^* denotes the representation *contragredient* or *dual* to the G -representation U on its dual space, in which for any functional φ in U^* , group element g in G and vector u in U , one has $g(\varphi)(u) = \varphi(g^{-1}(u))$. Cofixed spaces are dual to fixed spaces, as the following well-known proposition shows.

Proposition 3.3. *For any group G and any G -representation U over a field k , one has a k -vector space isomorphism $(U_G)^* \cong (U^*)^G$, in which U_G is the cofixed space for G acting on U , and $(U^*)^G$ is the subspace of G -fixed functionals in U^* .*

Proof. Recall that $U_G := U/N$ where N is the k -span of $\{g(u) - u\}_{u \in U, g \in G}$. Thus, by the universal property of quotients, $(U_G)^*$ is the subspace of functionals φ in U^* vanishing on restriction to N . This is equivalent to $0 = \varphi(g(u) - u) = \varphi(g(u)) - \varphi(u)$ for all u in U and g in G , that is, to φ lying in $(U^*)^G$. \square

Corollary 3.4. *For complementary degrees $i + j = d_0$ in $Q = S/\mathfrak{m}^{[q^m]}$, one has an \mathbb{F}_q -vector space duality of fixed and cofixed spaces $(Q_i^{P_\alpha})^* \cong (Q_j)_{P_\alpha}$, and hence equality of their dimensions. Therefore one has*

$$(3.6) \quad \text{Hilb}(Q_{P_\alpha}, t) = t^{d_0} \text{Hilb}(Q^{P_\alpha}, t^{-1}),$$

$$(3.7) \quad \text{Hilb}(S_{P_\alpha}, t) \equiv t^{d_0} \text{Hilb}(Q^{P_\alpha}, t^{-1}) \pmod{(t^{q^m})}, \quad \text{and}$$

$$(3.8) \quad \text{Hilb}(S_{P_\alpha}, t) = \lim_{m \rightarrow \infty} t^{d_0} \text{Hilb}(Q^{P_\alpha}, t^{-1}).$$

Proof. Equation (3.6) is immediate from the discussion surrounding Proposition 3.3. Then (3.6) implies (3.7), since the isomorphism (2.1) shows $(S_{P_\alpha})_d \cong (Q_{P_\alpha})_d$ for $0 \leq d \leq q^m - 1$. Lastly (3.7) implies (3.8). \square

Corollary 3.5. *Parabolic Conjecture 1.1 implies Parabolic Conjecture 1.2.*

Proof. Assuming Parabolic Conjecture 1.1, Equation (3.8) implies

$$\text{Hilb}(S_{P_\alpha}, t) = \lim_{m \rightarrow \infty} t^{d_0} \text{Hilb}(Q^{P_\alpha}, t^{-1}) = \lim_{m \rightarrow \infty} t^{d_0} C_{\alpha,m}(t^{-1}).$$

Hence Parabolic Conjecture 1.2 follows once one checks the following assertion:

$$(3.9) \quad t^{d_0} C_{\alpha,m}(t^{-1}) \equiv \sum_{\beta: \beta \leq \alpha} t^{\sum_{i=1}^{\ell} \alpha_i (q^{B_i} - 1)} \prod_{i=1}^{\ell} \prod_{j=0}^{\beta_i - 1} \frac{1}{1 - t^{q^{B_i} - q^{B_{i-1} + j}}} \pmod{(t^{q^m})}.$$

To prove (3.9), one first uses the definition (1.6) of $C_{\alpha,m}(t)$ to do a straightforward calculation showing

$$(3.10) \quad t^{d_0} C_{\alpha,m}(t^{-1}) = \sum_{\substack{\beta: \beta \leq \alpha \\ |\beta| \leq m}} t^{\sum_{i=1}^{\ell} \alpha_i (q^{B_i} - 1)} \frac{\prod_{j=0}^{|\beta| - 1} (1 - t^{q^m - q^j})}{\prod_{i=1}^{\ell} \prod_{j=0}^{\beta_i - 1} (1 - t^{q^{B_i} - q^{B_{i-1} + j}}}.$$

Since $q^{B_i} - 1 \geq q^{B_{i-1}}$, one has

$$\sum_{i=1}^{\ell} \alpha_i (q^{B_i} - 1) \geq \sum_{i=1}^{\ell} \alpha_i q^{B_{i-1}} \geq \alpha_{\ell} q^{B_{\ell} - 1} \geq q^{|\beta| - 1}.$$

This implies that for each $j = 0, 1, \dots, |\beta| - 1$ one has $(q^m - q^j) + \sum_{i=1}^{\ell} \alpha_i (q^{B_i} - 1) \geq q^m$. Therefore the right side in (3.10) is equivalent mod (t^{q^m}) to the right side in (3.9). \square

Corollary 3.6. *In the bivariate case $n = 2$, Parabolic Conjectures 1.1 and 1.2 are equivalent.*

Proof. Corollary 3.5 showed that Parabolic Conjecture 1.1 implies Parabolic Conjecture 1.2 for any n . The reverse implication when $n = 2$ arises when two coefficient comparisons valid for general n “meet in the middle”, as we now explain. Again, in this proof, all symbols “ \equiv ” mean congruence mod (t^q) . On one hand, one has

$$\text{Hilb}(Q^{P_\alpha}, t) \equiv \text{Hilb}(S^{P_\alpha}, t) = \prod_{i=1}^{\ell} \prod_{j=0}^{\alpha_i-1} \frac{1}{1 - t^{q^{A_i} - q^{A_{i-1} + j}}} \equiv C_{\alpha, m}(t)$$

where the left congruence is (2.2), the middle equality is (1.4), and the right congruence is Proposition 2.1. Therefore $\text{Hilb}(Q^{P_\alpha}, t)$ and $C_{\alpha, m}(t)$ have the same coefficients on $1, t, t^2, \dots, t^{q^m-1}$. On the other hand, one has

$$t^{d_0} \text{Hilb}(Q^{P_\alpha}, t^{-1}) \equiv \text{Hilb}(S_{P_\alpha}, t) = \sum_{\beta: \beta \leq \alpha} t^{\sum_{i=1}^{\ell} \alpha_i (q^{B_i} - 1)} \prod_{i=1}^{\ell} \prod_{j=0}^{\beta_i-1} \frac{1}{1 - t^{q^{B_i} - q^j}} \equiv t^{d_0} C_{\alpha, m}(t^{-1})$$

where the left congruence is (3.7), the middle equality is Parabolic Conjecture 1.2, and the right congruence is Corollary 3.9. Therefore $\text{Hilb}(Q^{P_\alpha}, t)$ and $C_{\alpha, m}(t)$ also have the same coefficients on $t^{d_0}, t^{d_0-1}, \dots, t^{d_0-(q^m-1)}$. Since $d_0 = n(q^m - 1)$, when $n = 2$, this means that $\text{Hilb}(Q^{P_\alpha}, t), C_{\alpha, m}(t)$ agree on *all* coefficients. \square

4. THE CASE WHERE m IS AT MOST 1

When $m = 0$, Parabolic Conjecture 1.1 says little: $Q = S/\mathfrak{m}^{[q^0]} = S/\mathfrak{m} = \mathbb{F}_q$ has no variables, so $Q^{P_\alpha} = Q = \mathbb{F}_q$ and $\text{Hilb}(Q^{P_\alpha}, t) = 1$. Meanwhile, $C_{\alpha, 0}(t) = 1$ since (1.6) has only the $\beta = 0$ summand.

The $m = 1$ case is less trivial.

Proposition 4.1. *Parabolic Conjecture 1.1 holds for $m = 1$.*

Proof. Given the composition $\alpha = (\alpha_1, \dots, \alpha_\ell)$ of n , the only weak compositions β with $0 \leq \beta \leq \alpha$ and $|\beta| \leq m = 1$ are $\beta = 0$ and $\beta = e_k = (0, \dots, 0, 1, 0, \dots, 0)$ for $k = 1, 2, \dots, \ell$. One therefore finds that

$$C_{\alpha, 1}(t) = t^{e(1, \alpha, 0)} \begin{bmatrix} 1 \\ 0, 1 \end{bmatrix}_{q, t} + \sum_{k=1}^{\ell} t^{e(1, \alpha, e_k)} \begin{bmatrix} 1 \\ e_k, 0 \end{bmatrix}_{q, t} = t^{n(q-1)} + \sum_{k=1}^{\ell} t^{A_{k-1}(q-1)} = \sum_{k=0}^{\ell} t^{A_k(q-1)},$$

recalling that $A_\ell = n$ and the convention that $A_0 = 0$. Thus to show $C_{\alpha, 1}(t) = \text{Hilb}(Q^{P_\alpha}, t)$, it will suffice to show that Q^{P_α} has \mathbb{F}_q -basis given by the images of the monomials

$$(4.1) \quad \{(x_1 x_2 \cdots x_{A_k})^{q-1}\}_{k=0, 1, \dots, \ell}.$$

To argue this, consider any polynomial

$$f(\mathbf{x}) = \sum_{\substack{a=(a_1, \dots, a_n) \\ a_i \in \{0, 1, \dots, q-1\}}} c_a \mathbf{x}^a$$

representing an element of the quotient $Q = S/\mathfrak{m}^{[q]}$. One has that $f(\mathbf{x})$ is invariant under the *diagonal matrices* T inside P_α if and only if each entry a_i is either 0 or $q-1$, that is, if $f(\mathbf{x})$ has the form

$$(4.2) \quad f(\mathbf{x}) = \sum_{A \subset \{1, 2, \dots, n\}} c_A \mathbf{x}_A^{q-1}$$

where $\mathbf{x}_A := \prod_{j \in A} x_j$, so that $\mathbf{x}_A^{q-1} = \prod_{j \in A} x_j^{q-1}$.

We claim that such an f is furthermore invariant under the *Borel subgroup* B of upper triangular matrices if and only if each monomial \mathbf{x}_A^{q-1} in the support of f has A forming an initial segment $A = \{1, 2, \dots, k\}$ for some k . To see this claim, note that B is generated by T together with $\{u_{ij} : 1 \leq i < j \leq n\}$ where u_{ij} sends $x_j \mapsto x_j + x_i$ and fixes all other variables x_ℓ with $\ell \neq j$. Working mod $\mathfrak{m}^{[q]}$ one checks that

$$u_{i,j}(\mathbf{x}_A^{q-1}) = \begin{cases} \mathbf{x}_A^{q-1} & \text{if } \{i, j\} \cap A \neq \{j\}, \\ \mathbf{x}_A^{q-1} + \mathbf{x}_{A \setminus \{j\} \cup \{i\}}^{q-1} & \text{if } \{i, j\} \cap A = \{j\}. \end{cases}$$

From this it is easily seen that each monomial $(x_1 x_2 \cdots x_k)^{q-1}$ has B -invariant image in Q . On the other hand, if $f(\mathbf{x})$ as in (4.2) has $c_A \neq 0$ for some A which is not an initial segment, then there exists $1 \leq i < j \leq n$ for which $\{i, j\} \cap A = \{j\}$, and one finds that $u_{i,j}(f) \neq f$, since $u_{i,j}(f) - f$ has coefficient c_A on $\mathbf{x}_{A \setminus \{j\} \cup \{i\}}^{q-1}$.

Lastly, an element of this more specific form $f(\mathbf{x}) = \sum_{k=0}^n c_k(x_1 x_2 \cdots x_k)^{q-1}$ will furthermore be invariant under the subgroup $\mathfrak{S}_{\alpha_1} \times \cdots \times \mathfrak{S}_{\alpha_\ell}$ of block permutation matrices inside P_α if and only if it is supported on the monomials in (4.1). Since P is generated by the Borel subgroup B together with this subgroup $\mathfrak{S}_{\alpha_1} \times \cdots \times \mathfrak{S}_{\alpha_\ell}$, the monomials in (4.1) give an \mathbb{F}_q -basis for Q^{P_α} . \square

5. THE COFIXED QUOTIENT S_G AS AN S^G -MODULE

Note that Parabolic Conjecture 1.2 has the following two consequences for the rational function $\frac{\text{Hilb}(S_{P_\alpha}, t)}{\text{Hilb}(S^{P_\alpha}, t)}$:

$$(5.1) \quad \frac{\text{Hilb}(S_{P_\alpha}, t)}{\text{Hilb}(S^{P_\alpha}, t)} \quad \text{lies in } \mathbb{Z}[t], \text{ and}$$

$$(5.2) \quad \lim_{t \rightarrow 1} \frac{\text{Hilb}(S_{P_\alpha}, t)}{\text{Hilb}(S^{P_\alpha}, t)} = 1.$$

The goal of the subsections below is to explain why (5.1), (5.2) do indeed hold, essentially due to three facts:

- (1) the P_α -cofixed quotient S_{P_α} is a finitely generated module over the P_α -invariant ring S^{P_α} ;
- (2) while S_{P_α} is *not* in general a free S^{P_α} -module, it does always have S^{P_α} -rank one; and
- (3) the P_α -invariant ring S^{P_α} is polynomial, as shown in [11, 17].

5.1. The cofixed spaces as a module over fixed subalgebra. Facts (1), (2) above hold generally for finite group actions, and are analogous to well-known facts about invariant rings. As we have not found them in the literature, we discuss them here.

Proposition 5.1. *Fix a field k , a k -algebra R , an R -module M , and let G be any subgroup of $\text{Aut}_R(M)$, the R -module automorphisms of M . Then one has that*

- (i) *the k -linear span N of all elements $\{g(m) - m\}_{g \in G, m \in M}$ is an R -submodule of M , and hence*
- (ii) *the cofixed space $M_G := M/N$ is a quotient R -module of M .*

Furthermore, if $\{m_i\}_{i \in I}$ generate M as an R -module, and if $\{g_j\}_{j \in J}$ generate G as a group, then

- (iii) *the images $\{\overline{m}_i\}_{i \in I}$ generate M_G as an R -module, and*
- (iv) *the elements $\{g_j^{\pm 1}(m_i) - m_i\}_{i \in I, j \in J}$ generate N as an R -module.*

Proof. All assertions are completely straightforward, except possibly for (iv), which relies on this calculation:

$$g_1 g_2(m) - m = g_1 g_2(m) - g_2(m) + g_2(m) - m$$

and the hypotheses let one express $g_2(m) = \sum_{i \in I} r_i m_i$ for some r_i in R , so that one can rewrite this as

$$g_1 g_2(m) - m = \sum_{i \in I} r_i (g_1(m_i) - m_i) + (g_2(m) - m). \quad \square$$

Corollary 5.2. *Let S be a finitely generated k -algebra and G a finite subgroup of k -algebra automorphisms of S , e.g., $S = k[x_1, \dots, x_n]$ and G a finite subgroup of $GL_n(k)$ acting by linear substitutions.*

Then the G -cofixed space S_G is a finitely generated module over the G -fixed subalgebra S^G .

Proof. Via Proposition 5.1(ii,iii), it suffices to show that S is a finitely generated S^G -module. This is well-known argument via [3, Cor. 5.2]; see [5, Thm. 1.3.1], [23, Thm. 2.3.1]. One has that S is integral over S^G , as any x in S satisfies the monic polynomial $\prod_{g \in G} (t - g(x))$ in $S^G[t]$, and S is finitely generated as an algebra over S^G because it is finitely generated as a k -algebra. \square

Example 5.3. In the case of $M = S = \mathbb{F}_q[x_1, \dots, x_n]$ and $G = GL_n(\mathbb{F}_q)$, one has that S is even a *free* S^G -module of rank $|G|$ with an explicit S^G -basis of monomials $\{x^\alpha\}_{0 \leq \alpha_i \leq q^n - q^{i-1} - 1}$ provided by Steinberg [25] in his proof of Dickson's Theorem. Consequently, S_G is generated by the images of these monomials, and Proposition 5.1(iv) leads to an explicit finite presentation of S_G as a quotient of the free S^G -module S , useful for computations.

Corollary 5.4. *When a finite subgroup G of $GL_n(k)$ acting by linear substitutions on $S = k[x_1, \dots, x_n]$ has G -fixed subalgebra S^G which is again a polynomial algebra, then $\text{Hilb}(S_G, t)/\text{Hilb}(S^G, t)$ lies in $\mathbb{Z}[t]$.*

Proof. When S^G is polynomial, the *Hilbert syzygy theorem* (see e.g. [5, §2.1], [23, §6.3]) implies that S_G will have a finite S^G -free resolution $0 \rightarrow F_n \rightarrow \cdots \rightarrow F_1 \rightarrow F_0 \rightarrow S_G \rightarrow 0$ where $F_i = \bigoplus_{j \geq 0} S^G(-j)^{\beta_{i,j}}$ for some nonnegative integers $\beta_{i,j}$. Here $R(-j)$ denotes a copy of the graded ring R , regarded as a module over itself, but with grading shift so that the unit 1 is in degree j , so that $\text{Hilb}(F_i, t) = \text{Hilb}(S^G, t) \cdot \sum_{j \geq 0} \beta_{i,j} t^j$. Considering Euler characteristics in each homogeneous component of the resolution gives

$$\text{Hilb}(S^G, t) \sum_{i,j \geq 0} (-1)^i \beta_{i,j} t^j = \text{Hilb}(S_G, t)$$

so that $\text{Hilb}(S_G, t) / \text{Hilb}(S^G, t) = \sum_{i,j \geq 0} (-1)^i \beta_{i,j} t^j$ lies in $\mathbb{Z}[t]$. \square

5.2. The cofixed space is a rank one module. We next explain, via consideration of the rank of S_G as an S^G -module, why one should expect (5.2) to hold.

Definition 5.5. Recall [8, §12.1] for a finitely generated M over an integral domain R , that $\text{rank}_R(M)$ is the maximum size of an R -linearly independent subset of M .

Alternatively, $\text{rank}_R(M)$ is the largest integer r such that M contains a free R -submodule R^r , and in this situation, the quotient M/R^r will be all R -torsion, that is, for every x in M/R^r there exists some $a \neq 0$ in R with $ax = 0$. One can equivalently define this using the *field of fractions* $K := \text{Frac}(R)$ via

$$(5.3) \quad \text{rank}_R(M) := \dim_K (K \otimes_R M).$$

Indeed, clearing denominators shows that a subset $\{m^{(i)}\} \subset M$ is R -linearly independent if and only if $\{1 \otimes m^{(i)}\} \subset K \otimes_R M$ is K -linearly independent.

In the graded setting, one has the following well-known characterization of rank via Hilbert series.

Proposition 5.6. *For R an integral domain which is also a finitely generated graded k -algebra, and M a finitely generated graded R -module, the rational functions $\text{Hilb}(R, t)$ and $\text{Hilb}(M, t)$ satisfy*

$$\text{rank}_R(M) = \lim_{t \rightarrow 1} \frac{\text{Hilb}(M, t)}{\text{Hilb}(R, t)}.$$

Proof. Letting $r := \text{rank}_R(M)$, we claim that one can choose an R -linearly independent subset of size r in M consisting of *homogeneous* elements as follows. Given *any* R -linearly independent subset $\{m^{(i)}\}_{i=1,2,\dots,r}$, decompose them into their homogeneous components $m^{(i)} = \sum_j m_j^{(i)}$. Then the set of all such components $\{m_j^{(i)}\}$ spans an R -submodule of M containing the R -submodule spanned by $\{m^{(i)}\}_{i=1,2,\dots,r}$. Thus the set of all such components must contain an R -linearly independent subset of size r .

Now consider the free R -submodule $R^r := \bigoplus_{i=1}^r R m_i$ spanned by a homogeneous R -linearly independent subset $\{m_i\}_{i=1,2,\dots,r}$, so that the quotient M/R^r will be all R -torsion. Then

$$\lim_{t \rightarrow 1} \frac{\text{Hilb}(M, t)}{\text{Hilb}(R, t)} = \lim_{t \rightarrow 1} \frac{\text{Hilb}(R^r, t)}{\text{Hilb}(R, t)} + \lim_{t \rightarrow 1} \frac{\text{Hilb}(M/R^r, t)}{\text{Hilb}(R, t)}.$$

Since $\text{Hilb}(R^r, t) / \text{Hilb}(R, t) = \sum_{i=1}^r t^{\deg(m_i)}$, the first limit on the right is r . One argues that the second limit on the right vanishes as follows. Assume R has Krull dimension d , that is, $\text{Hilb}(R, t)$ has a pole of order d at $t = 1$. Thus one must show that $\text{Hilb}(M/R^r, t)$ has its pole of order at most $d - 1$. To this end, choose homogeneous generators y_1, \dots, y_N for the R -torsion module M/R^r , say with $\theta_i y_i = 0$ for nonzero homogeneous θ_i in R . Then one has a graded R -module surjection $\bigoplus_{i=1}^N R/(\theta_i)(-\deg(y_i)) \twoheadrightarrow M/R^r$ sending the basis element of $R/(\theta_i)$ to y_i . This gives a coefficientwise inequality

$$(5.4) \quad \text{Hilb}(M/R^r, t) \leq \sum_{i=1}^N t^{\deg(y_i)} \text{Hilb}(R/(\theta_i), t) = \sum_{i=1}^N (1 - t^{\deg(\theta_i)}) t^{\deg(y_i)} \text{Hilb}(R, t)$$

between power series with nonnegative coefficients, which are also rational functions having poles confined to the unit circle. As each summand on the right of (5.4) has a pole of order at most $d - 1$ at $t = 1$, the same holds for $\text{Hilb}(M/R^r, t)$. \square

For a subgroup G of ring automorphisms of the domain S , denote by $K := \text{Frac}(S)^G$ the G -invariant subfield of $L := \text{Frac}(S)$. When G is finite, an easy argument [5, Prop. 1.1.1], [23, Prop. 1.2.4] shows that

$$K := \text{Frac}(S^G) = \text{Frac}(S)^G (= L^G),$$

giving this commuting diagram of inclusions

$$(5.5) \quad \begin{array}{ccc} S & \hookrightarrow & L \\ \uparrow & & \uparrow \\ S^G & \hookrightarrow & K \end{array}$$

Consequently, Proposition 5.6 together with the next result immediately imply (5.2).

Proposition 5.7. *A finite group G of automorphisms of an integral domain S has $\text{rank}_{S^G} S_G = 1$.*

Proof. Using (5.3) to characterize rank, it suffices to show this chain of three K -vector space isomorphisms:

$$(5.6) \quad K \otimes_{S^G} S_G \cong L_G \cong (KG)_G \cong K.$$

For the first step in (5.6), start with the short exact sequence that defines S_G

$$0 \longrightarrow \sum_{\substack{g \in G \\ s \in S}} S^G(g(s) - s) \longrightarrow S \longrightarrow S_G \longrightarrow 0$$

and apply the exact localization functor $K \otimes_{S^G} (-)$ to give the short exact sequence

$$(5.7) \quad 0 \longrightarrow \sum_{\substack{g \in G \\ s \in S}} K \otimes_{S^G} S^G(g(s) - s) \longrightarrow K \otimes_{S^G} S \longrightarrow K \otimes_{S^G} S_G \longrightarrow 0$$

Using the K -vector space isomorphism $K \otimes_{S^G} S \cong L$ induced by $f \otimes s \mapsto fs$, the sequence (5.7) becomes

$$0 \longrightarrow \sum_{\substack{g \in G \\ f \in L}} K(g(f) - f) \longrightarrow L \longrightarrow K \otimes_{S^G} S_G \longrightarrow 0$$

which shows that $K \otimes_{S^G} S_G \cong L_G$, completing the first step.

The second step in (5.6) comes from considering the Galois extension $K = L^G \hookrightarrow L$ having Galois group G , that appears as the right vertical map in (5.5). The Normal Basis Theorem of Galois Theory [16, Theorem 13.1] asserts that, not only is $L \cong K^{|G|}$ as a K -vector space, but L is even isomorphic to the *left-regular representation* KG as KG -module. Hence $L_G \cong (KG)_G$, completing the second step.

The third step in (5.6) comes from the short exact sequence of KG -modules

$$(5.8) \quad 0 \longrightarrow I_G \longrightarrow KG \xrightarrow{\epsilon} K \longrightarrow 0.$$

Here G acts trivially on K , while the *augmentation ideal* I_G is the kernel of the *augmentation map* ϵ sending each K -basis element g of KG to 1 in K . Since I_G is K -spanned by $g - h$ for g, h in G , the sequence (5.8) shows that $(KG)_G \cong K$, completing the third step. \square

This immediately implies the following corollary, explaining (5.2).

Corollary 5.8. *When a finite subgroup G of $GL_n(k)$ acting by linear substitutions on $S = k[x_1, \dots, x_n]$ has G -fixed subalgebra S^G which is again a polynomial algebra, then*

$$\lim_{t \rightarrow 1} \frac{\text{Hilb}(S_G, t)}{\text{Hilb}(S^G, t)} = \text{rank}_{S^G} S_G = 1.$$

5.3. A conjecture on the module structure of the G -cofixed space. Computer experimentation suggests the following conjecture on the S^G -module structure of S_G for $G = GL_n(\mathbb{F}_q)$.

Recall that $S^G = \mathbb{F}_q[D_{n,0}, D_{n,1}, \dots, D_{n,n-1}]$ where the Dickson polynomials $D_{n,i}$ were defined in the introduction. Consider subalgebras of S^G defined for $i = 1, 2, \dots, n$ by

$$\mathbb{F}_q[Z_i] := \mathbb{F}_q[D_{n,n-i}, D_{n,n-i+1}, \dots, D_{n,n-2}, D_{n,n-1}].$$

Conjecture 5.9. *There is a subset M of homogeneous elements minimally generating S_G as an S^G -module, with a decomposition $M = \bigsqcup_{i=1}^n M_i$ having the following properties.*

- The $\mathbb{F}_q[Z_i]$ -submodule generated by M_i within S_G is $\mathbb{F}_q[Z_i]$ -free.
- The Dickson polynomials $D_{n,0}, D_{n,1}, \dots, D_{n,n-i-1}$ not in $\mathbb{F}_q[Z_i]$ all annihilate every element of M_i .
- The last set M_n is a singleton, whose unique element has degree $(n-1)(q^n - 1)$.

Note that this conjecture implies a Hilbert series expansion of the form

$$(5.9) \quad \text{Hilb}(S_G, t) = \sum_{i=1}^n \frac{\sum_{m \in M_i} t^{\deg(m)}}{(1 - t^{q^n - q^{n-1}})(1 - t^{q^n - q^{n-2}}) \cdots (1 - t^{q^n - q^{n-i}})}.$$

Example 5.10. In the case $n = 1$, Example 1.3 shows that S_G is a free S^G -module of rank 1 with basis element given by the image of 1. Therefore Conjecture 5.9 holds in this case by taking $M = M_1 = \{1\}$.

Example 5.11. When $n = 2$, Theorem B.15 below will confirm Conjecture 5.9 taking $M = M_1 \sqcup M_2$ where $M_1 = \{1, XY, X^2Y, \dots, X^{q-2}Y\}$ and $M_2 = \{X^qY\}$ with $X := x^{q-1}, Y := y^{q-1}$.

Example 5.12. Conjecture 5.9 has also been checked by D. Stamate for $n = 3$ and $q = 2, 3, 4, 5$ using *Singular*. Using the abbreviation $T := t^{q-1}$, the expansions of $\text{Hilb}(S_G, t)$ as in (5.9) are as follows: for $q = 2$,

$$\frac{1}{1 - T^4} + \frac{T^3 + T^5 + T^6}{(1 - T^4)(1 - T^6)} + \frac{T^{14}}{(1 - T^4)(1 - T^6)(1 - T^7)};$$

for $q = 3$,

$$\frac{1 + T^3 + T^5 + T^6}{1 - T^9} + \frac{T^4 + T^7 + T^8 + T^{10} + T^{11} + T^{12} + T^{15} + T^{18}}{(1 - T^9)(1 - T^{12})} + \frac{T^{26}}{(1 - T^9)(1 - T^{12})(1 - T^{13})};$$

for $q = 4$,

$$\begin{aligned} & \frac{T^0 + T^3 + T^4 + T^6 + T^7 + T^8 + T^{11} + T^{12} + T^{14} + T^{15}}{1 - T^{16}} \\ & + \frac{T^5 + T^9 + T^{10} + T^{13} + T^{15} + T^{17} + T^{18} + T^{19} + T^{20} + T^{23} + T^{24} + T^{27} + T^{28} + T^{32} + T^{34}}{(1 - T^{16})(1 - T^{20})} \\ & + \frac{T^{42}}{(1 - T^{16})(1 - T^{20})(1 - T^{21})}; \end{aligned}$$

and for $q = 5$,

$$\begin{aligned} & \frac{T^0 + T^3 + T^4 + T^5 + T^7 + T^8 + T^9 + T^{10} + T^{13} + T^{14} + T^{15} + T^{18} + T^{19} + T^{20} + T^{23} + T^{24}}{1 - T^{25}} \\ & + \frac{1}{(1 - T^{25})(1 - T^{30})} \cdot \left(T^6 + T^{11} + T^{12} + T^{16} + T^{17} + T^{18} + T^{21} + T^{22} + T^{23} + T^{24} + T^{26} + T^{27} + T^{28} \right. \\ & \quad \left. + T^{29} + T^{30} + T^{33} + T^{34} + T^{35} + T^{38} + T^{39} + T^{40} + T^{44} + T^{45} + T^{50} \right) \\ & \quad + \frac{T^{62}}{(1 - T^{25})(1 - T^{30})(1 - T^{31})}. \end{aligned}$$

Remark 5.13. Conjecture 5.9 is reminiscent of the *Landweber-Stong Conjecture* in modular invariant theory, proven when $q = p$ is prime by Bourguiba and Zarati [6]:

Conjecture 5.14 (Landweber and Stong [15]). *For a subgroup H of $GL_n(\mathbb{F}_q)$ acting on $S = \mathbb{F}_q[\mathbf{x}]$, the depth of the H -invariant ring S^H is the maximum i for which the elements $D_{n,n-i}, D_{n,n-i+1}, \dots, D_{n,n-2}, D_{n,n-1}$ form a regular sequence on S^H .*

Remark 5.15. One might ask why Conjecture 5.9 has been formulated only for G , and not for all parabolic subgroups P_α of G . In fact, Theorem B.10 below does prove such a result for $n = 2$, when there is only one proper parabolic subgroup, the Borel subgroup $B = P_{(1,1)}$ inside $G = GL_2(\mathbb{F}_q)$.

However, computer calculations in **Sage** suggest that a naive formulation of such a conjecture fails generally. Specifically, for $n = 3$ and $q = 4$ with $B = P_{(1,1,1)}$ inside $G = GL_3(\mathbb{F}_4)$, one encounters the following difficulty. One wants a minimal generating set M for S_B as an S^B -module of a particular form. Note that here $S^B = \mathbb{F}_4[f_3, f_{12}, f_{48}]$, where $f_3 := x^3$, $f_{12} := \prod_{c \in \mathbb{F}_4} (y + cx)^3 = y^{12} + x^3y^9 + x^6y^6 + x^9y^3$, and $f_{48} := D_{3,2}(x, y, z)$. One can also show, using the idea in [12, §2.1] and Proposition B.8 below, that f_{48} acts as a nonzero-divisor on S_B . Thus one might expect a decomposition of the minimal generators as

$$(5.10) \quad M = M_1 \sqcup M_2 \sqcup M_3 \sqcup M_4$$

in which

- $\mathbb{F}_4[f_3, f_{12}, f_{48}]$ acts freely on M_4 ,
- $\mathbb{F}_4[f_{12}, f_{48}]$ acts freely on M_3 , but f_3 annihilates it,
- $\mathbb{F}_4[f_3, f_{48}]$ acts freely on M_2 , but f_{12} annihilates it, and
- $\mathbb{F}_4[f_{48}]$ acts freely on M_1 , but both f_3, f_{12} annihilate it.

We argue this is impossible as follows. Let $(S_B)_{\leq d} := \bigoplus_{i=0}^d (S_B)_i$, and similarly $(S_B)_{< d} := \bigoplus_{i=0}^{d-1} (S_B)_i$. Given a subset $A \subset S_B$, let $S^B A$ denote the S^B -submodule of S_B that it generates. Then computations show $\text{Hilb}(S^B(S_B)_{\leq 42}, t) - \text{Hilb}(S^B(S_B)_{< 42}, t)$ agrees up through degree 90 with

$$t^{42} \cdot \text{Hilb}(\mathbb{F}_4[f_3, f_{48}], t) + t^{42} \cdot \text{Hilb}(\mathbb{F}_4[f_{12}, f_{48}], t).$$

One can check that this would force that in any decomposition (5.10), the sets M_2, M_3 must each contain exactly one element of degree 42. But computations show that for every element f in $(S_B)_{42}$, the difference

$$\text{Hilb}(S^B((S_B)_{< 42} \cup \{f\}), t) - \text{Hilb}(S^B(S_B)_{< 42}, t)$$

is neither equal to $t^{42} \text{Hilb}(\mathbb{F}_4[f_3, f_{48}], t)$, nor to $t^{42} \text{Hilb}(\mathbb{F}_4[f_{12}, f_{48}], t)$. Thus there are no suitable choices for these elements of M_2, M_3 .

6. COMPARING TWO REPRESENTATIONS

This section reveals the original motivation for our conjectures, analogous to questions on real and complex reflection groups W , their *parking spaces*, *W-Catalan numbers*, and *Fuss-Catalan* generalizations. We refer the reader to [2, 20] for the full story on this analogy; see also Section 7.4 below. Roughly speaking, we start by examining two strikingly similar G -representations, that we will call the *graded* and *ungraded G-parking spaces*. Parabolic Conjecture 1.1 turns out to yield a comparison of their P_α -fixed subspaces.

6.1. The graded and ungraded $GL_n(\mathbb{F}_q)$ -parking spaces.

Definition 6.1. For a field $k \supset \mathbb{F}_q$, the *graded parking space* for $G = GL_n(\mathbb{F}_q)$ over k is

$$Q_k := k \otimes_{\mathbb{F}_q} Q = k[x_1, \dots, x_n] / (x_1^{q^m}, \dots, x_n^{q^m}) = S_k / \mathfrak{m}^{[q^m]}$$

where $S_k := k[x_1, \dots, x_n]$ and $\mathfrak{m} := (x_1, \dots, x_n)$. The group $G = GL_n(\mathbb{F}_q) \subset GL_n(k)$ acts on S_k via linear substitutions, and also on Q_k , just as before. Thus Q_k is a graded kG -module.

Definition 6.2. For a field $k \supset \mathbb{F}_q$, the *ungraded parking space*

$$k[\mathbb{F}_{q^m}^n] := \text{span}_k \{e_v : v \in \mathbb{F}_{q^m}^n\}$$

for G over k is the G -permutation representation on the points of $\mathbb{F}_{q^m}^n$ via the embedding $G = GL_n(\mathbb{F}_q) \subset GL_n(\mathbb{F}_{q^m})$, considered as a kG -module. In other words, the element g in $G = GL_n(\mathbb{F}_q)$ represented by a matrix (g_{ij}) will send the k -basis element e_v indexed by $v = (v_1, \dots, v_n)$ in $\mathbb{F}_{q^m}^n$ to $g(e_v) = e_{g(v)}$, where $g(v)_i = \sum_{j=1}^n g_{ij} v_j$.

Example 6.3. When $q = 3, n = 2, m = 1$, the ungraded parking space has these nine k -basis elements:

$$\left\{ \begin{array}{ccc} e_{(-1,+1)}, & e_{(0,+1)}, & e_{(+1,+1)}, \\ e_{(-1,0)}, & e_{(0,0)}, & e_{(+1,0)}, \\ e_{(-1,-1)}, & e_{(0,-1)}, & e_{(+1,-1)} \end{array} \right\}.$$

For example, $-I_{2 \times 2}$ in $G = GL_2(\mathbb{F}_3)$ fixes $e_{(0,0)}$ and swaps the remaining basis elements as follows:

$$\begin{array}{ccc} e_{(-1,0)} & \leftrightarrow & e_{(+1,0)} \\ e_{(-1,+1)} & \leftrightarrow & e_{(+1,-1)} \\ e_{(0,+1)} & \leftrightarrow & e_{(0,-1)} \\ e_{(+1,+1)} & \leftrightarrow & e_{(-1,-1)}. \end{array}$$

Note that both kG -modules Q_k and $k[\mathbb{F}_{q^m}^n]$ have dimension $(q^m)^n$. Before investigating their further similarities, we first note that they are *not in general isomorphic* for $n \geq 2$.

Example 6.4. As in Example 6.3, take $q = 3, n = 2, m = 1$. One can argue that

$$Q_k = k[x_1, x_2]/(x_1^3, x_2^3) \not\cong k[\mathbb{F}_3^2]$$

as follows. The action of $G = GL_2(\mathbb{F}_3)$ commutes with the action of its center $C = \{\pm I_{2 \times 2}\} \cong \mathbb{Z}/2\mathbb{Z}$. Thus a kG -module isomorphism $Q_k \cong k[\mathbb{F}_3^2]$ would necessarily lead to a $k[G \times C]$ -module isomorphism, and hence also kG -module isomorphisms between the C -isotypic subspaces Q_k^- and $k[\mathbb{F}_3^2]^-$ where for $U = Q_k$ or $k[\mathbb{F}_3^2]$ we define

$$U^- := \{u \in U \text{ such that } -I_{2 \times 2} : u \mapsto -u\}.$$

It therefore suffices to check that these two isotypic subspaces are *not* kG -module isomorphic:

$$\begin{aligned} Q_k^- &= \{f \in Q_k : f(-x_1, -x_2) = -f(x_1, x_2)\} = (Q_k)_1 \oplus (Q_k)_3 \\ &= \text{span}_k \left\{ \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \right\} \oplus \text{span}_k \left\{ \begin{pmatrix} x_1^2 x_2 \\ x_1 x_2^2 \end{pmatrix} \right\}, \end{aligned}$$

$$\begin{aligned} k[\mathbb{F}_3^2]^- &= \{w \in k[\mathbb{F}_3^2] : -I_{2 \times 2} : w \mapsto -w\} \\ &= \text{span}_k \left\{ \begin{aligned} w_1 &:= e_{(+1,0)} - e_{(-1,0)}, \\ w_2 &:= e_{(0,+1)} - e_{(0,-1)}, \\ w_3 &:= e_{(+1,+1)} - e_{(-1,-1)}, \\ w_4 &:= e_{(-1,+1)} - e_{(+1,-1)} \end{aligned} \right\}. \end{aligned}$$

To argue that $Q_k^- \not\cong k[\mathbb{F}_3^2]^-$ as kG -modules, check that this transvection in G

$$u = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

acts on both of the 2-dimensional summands $(Q_k)_1$ and $(Q_k)_3$ of Q_k^- via 2×2 Jordan blocks, but it acts on the 4-dimensional space $k[\mathbb{F}_3^2]^-$ by fixing w_1 and cyclically permuting $w_2 \mapsto w_3 \mapsto w_4 \mapsto w_2$. This 3-cycle action is conjugate to a 3×3 Jordan block when k has characteristic 3.

Although Q_k and $k[\mathbb{F}_{q^m}^n]$ are not *isomorphic* as kG -modules, they do turn out to be *Brauer isomorphic*.

Definition 6.5. Recall [22, Chapter 18] that two finite-dimensional representations U_1, U_2 of a finite group G over a field k are said to be *Brauer-isomorphic* as kG -modules, written $U_1 \approx U_2$, if each simple kG -module has the same composition multiplicity in U_1 as in U_2 . Equivalently, each p -regular element g in G has the same *Brauer character values* $\chi_{U_1}(g) = \chi_{U_2}(g)$.

In fact, when the field extension k of \mathbb{F}_q actually contains \mathbb{F}_{q^m} , it is useful to consider an extra cyclic group

$$C := \mathbb{F}_{q^m}^\times \cong \mathbb{Z}/(q^m - 1)\mathbb{Z}$$

acting on both Q_k and $k[\mathbb{F}_{q^m}^n]$ in a way that commutes with the G -actions.

Definition 6.6 (C -action on the graded parking space). When $k \supset \mathbb{F}_{q^m}$, an element γ in $C = \mathbb{F}_{q^m}^\times$ acts on $S_k = k[x_1, \dots, x_n]$ by the scalar variable substitution

$$x_i \mapsto \gamma x_i \text{ for } i = 1, 2, \dots, n.$$

This C -action preserves $\mathbf{m}^{[q^m]} = (x_1^{q^m}, \dots, x_n^{q^m})$, so that it descends to a C -action on Q_k . Also this C -action commutes with the action of G , so that Q_k becomes a $k[G \times C]$ -module.

Note that the C -action on Q_k depends in a trivial way on the *grading* structure of Q_k : an element γ of $C = \mathbb{F}_{q^m}^\times$ scales all elements of a fixed degree d in Q_k by the same scalar γ^d .

Definition 6.7 (C -action on the ungraded parking space). When $k \supset \mathbb{F}_{q^m}$, an element γ in $C = \mathbb{F}_{q^m}^\times$ permutes the elements of $\mathbb{F}_{q^m}^n$ via diagonal scalings:

$$v = (v_1, \dots, v_n) \xrightarrow{\gamma} (\gamma v_1, \dots, \gamma v_n).$$

Again this commutes with the permutation action of G on $\mathbb{F}_{q^m}^n$, giving $k[\mathbb{F}_{q^m}^n]$ the structure of a permutation $k[G \times C]$ -module.

To understand why the $k[G \times C]$ -modules Q_k and $k[\mathbb{F}_{q^m}^n]$ are Brauer-isomorphic, we introduce a third object: an ungraded ring R_k that turns out to be a thinly disguised version of $k[\mathbb{F}_{q^m}^n]$.

Definition 6.8. Define an ungraded quotient ring R_k of $S_k = k[x_1, \dots, x_n]$ by

$$R_k := S_k / \mathfrak{n} \quad \text{where} \quad \mathfrak{n} := (x_1^{q^m} - x_1, \dots, x_n^{q^m} - x_n).$$

As \mathfrak{n} is stable under the $G \times C$ -action on S_k , the quotient R_k inherits the structure of a $k[G \times C]$ -module.

Proposition 6.9. *When $k \supset \mathbb{F}_{q^m}$, one has a $k[G \times C]$ -module isomorphism $R_k \cong k^{\mathbb{F}_{q^m}^n}$, where $k^{\mathbb{F}_{q^m}^n}$ is the ring of all k -valued functions on the finite set $\mathbb{F}_{q^m}^n$ with pointwise addition and multiplication. In particular, R_k is $k[G \times C]$ -module isomorphic to the contragredient of $k[\mathbb{F}_{q^m}^n]$, and hence to $k[\mathbb{F}_{q^m}^n]$ itself.*

Proof. The map $S_k \rightarrow k^{\mathbb{F}_{q^m}^n}$ that evaluates a polynomial $f(x_1, \dots, x_n)$ at the points of $\mathbb{F}_{q^m}^n$ is well-known to be a surjective ring homomorphism with kernel \mathfrak{n} when $k \supset \mathbb{F}_{q^m}$. This proves most of the assertions. For the last assertion, note that permutation representations are self-contragredient. \square

It will turn out that S_k is closely related to R_k via a filtration

$$(6.1) \quad F_0 \subset F_1 \subset F_2 \subset \dots \subset R_k$$

where F_i is the image within R_k of polynomials in S_k of degree at most i . Note that $F_i F_j \subset F_{i+j}$, allowing one to define the *associated graded ring*

$$\mathfrak{gr}_F R_k := F_0 \oplus F_1/F_0 \oplus F_2/F_1 \oplus F_3/F_2 \oplus \dots$$

with multiplication $F_i/F_{i-1} \times F_j/F_{j-1} \rightarrow F_{i+j}/F_{i+j-1}$ induced from $F_i \times F_j \rightarrow F_{i+j}$.

Proposition 6.10. *When $k \supset \mathbb{F}_{q^m}$, one has a $G \times C$ -equivariant isomorphism of graded rings $Q_k \cong \mathfrak{gr}_F R_k$.*

Proof. Consider the k -algebra map φ defined by

$$(6.2) \quad \begin{array}{ccc} S_k & \xrightarrow{\varphi} & \mathfrak{gr}_F R_k \\ x_i & \mapsto & \bar{x}_i \end{array} \in F_1/F_0.$$

We claim φ is surjective: R_k is generated as a k -algebra by the images of x_1, \dots, x_n , so the multiplication map

$$\underbrace{F_1 \times \dots \times F_1}_{i \text{ factors}} \rightarrow F_i$$

is surjective, and hence likewise for the induced multiplication map $F_1/F_0 \times \dots \times F_1/F_0 \rightarrow F_i/F_{i-1}$.

The relation $x_i^{q^m} = x_i$ that holds in R_k shows that $\bar{x}_i^{q^m} = \bar{x}_i = 0$ inside the q^m -graded component F_{q^m}/F_{q^m-1} of $\mathfrak{gr}_F R_k$. Hence the surjection $S_k \xrightarrow{\varphi} \mathfrak{gr}_F R_k$ has $\mathfrak{m}^{[q^m]}$ in its kernel, and descends to a surjection $Q_k \xrightarrow{\varphi} \mathfrak{gr}_F R_k$. But all of Q_k , R_k , $\mathfrak{gr}_F R_k$ have dimension $(q^m)^n$, so φ is an isomorphism. Furthermore, it is easily seen to be $G \times C$ -equivariant. \square

Corollary 6.11. *When $k \supset \mathbb{F}_q$, one has a Brauer-isomorphism of kG -modules $Q_k \approx k[\mathbb{F}_{q^m}^n]$.*

If furthermore $k \supset \mathbb{F}_{q^m}$ then it is a Brauer-isomorphism of $k[G \times C]$ -modules.

Proof. One may assume without loss of generality that $k \supset \mathbb{F}_{q^m}$, as one has Brauer-isomorphisms between two kG -modules if and only if the same holds after extending scalars to any field containing k .

Then one has a string of $k[G \times C]$ -module Brauer isomorphisms and isomorphisms

$$k[\mathbb{F}_{q^m}^n] \cong R_k \approx \mathfrak{gr}_F R_k \cong Q_k$$

derived, respectively, from Proposition 6.9, from the filtration defining $\mathfrak{gr}_F R_k$, and from Proposition 6.10. \square

6.2. P_α -fixed spaces, orbits, and Parabolic Conjecture 1.1. We next compare the P_α -fixed spaces in Q_k and in $k[\mathbb{F}_{q^m}^n]$. Since $k[\mathbb{F}_{q^m}^n]$ is a permutation representation, one can identify its fixed space as

$$k[\mathbb{F}_{q^m}^n]^{P_\alpha} \cong k[P_\alpha \backslash \mathbb{F}_{q^m}^n]$$

where $P_\alpha \backslash \mathbb{F}_{q^m}^n$ is the set of P_α -orbits on $\mathbb{F}_{q^m}^n$. This orbit set $P_\alpha \backslash \mathbb{F}_{q^m}^n$ turns out to be closely related to the mysterious summation in the definition (1.6) of $C_{\alpha,m}(t)$.

Definition 6.12. Let $\beta = (\beta_1, \dots, \beta_\ell)$ be a weak composition having $|\beta| \leq m$, and define its partial sums $B_i = \beta_1 + \beta_2 + \dots + \beta_i$ as usual. A $(\beta, m - |\beta|)$ -flag in \mathbb{F}_{q^m} is a tower

$$(6.3) \quad 0 = V_{B_0} \subset V_{B_1} \subset V_{B_2} \subset \dots \subset V_{B_\ell} \subset \mathbb{F}_{q^m}$$

of \mathbb{F}_q -subspaces inside \mathbb{F}_{q^m} with $\dim_{\mathbb{F}_q} V_{B_i} = B_i$ for each i .

Let Y_β be the set of $(\beta, m - |\beta|)$ -flags in \mathbb{F}_{q^m} , whose cardinality is known to be a q -multinomial coefficient

$$|Y_\beta| = \left[\begin{matrix} m \\ \beta, m - |\beta| \end{matrix} \right]_q := \left[\begin{matrix} m \\ \beta, m - |\beta| \end{matrix} \right]_{q,t=1} = \frac{\prod_{j=0}^{n-1} (q^n - q^j)}{\prod_{i=1}^\ell \prod_{j=0}^{\beta_i-1} (q^{B_i} - q^{B_{i-1}+j})}.$$

Given a composition α of n , define the set

$$X_\alpha := \bigsqcup_{\substack{\beta: \beta \leq \alpha, \\ |\beta| \leq m}} Y_\beta,$$

which has cardinality given by

$$|X_\alpha| = \sum_{\substack{\beta: \beta \leq \alpha, \\ |\beta| \leq m}} |Y_\beta| = [C_{\alpha,m}(t)]_{t=1}.$$

Theorem 6.13. *The set X_α naturally indexes $P_\alpha \backslash \mathbb{F}_{q^m}^n$. Therefore*

$$\dim_k k[\mathbb{F}_{q^m}^n]^{P_\alpha} = |P_\alpha \backslash \mathbb{F}_{q^m}^n| = [C_{\alpha,m}(t)]_{t=1}.$$

Proof. Fix $\alpha = (\alpha_1, \dots, \alpha_\ell)$ and denote its partial sums by $A_i = \alpha_1 + \alpha_2 + \dots + \alpha_i$ as usual. To any vector $v = (v_1, \dots, v_n)$ in $\mathbb{F}_{q^m}^n$ one can associate a flag $(V_i)_{i=1}^\ell$ in \mathbb{F}_{q^m} defined by $V_i := \text{span}_{\mathbb{F}_q} \{v_1, v_2, \dots, v_{A_i}\}$. This gives rise to a weak composition $\beta = (\beta_1, \dots, \beta_\ell)$ with

$$\beta_i = \dim_{\mathbb{F}_q} V_i - \dim_{\mathbb{F}_q} V_{i-1} = \dim_{\mathbb{F}_q} V_i / V_{i-1} \leq \alpha_i,$$

where the inequality arises because V_i / V_{i-1} is spanned by the α_i vectors $\{v_{A_{i-1}+1}, v_{A_{i-1}+2}, \dots, v_{A_i}\}$. Also one has

$$|\beta| = \dim_{\mathbb{F}_q} \text{span}_{\mathbb{F}_q} \{v_1, v_2, \dots, v_n\} \leq \dim_{\mathbb{F}_q} \mathbb{F}_{q^m} = m.$$

Thus the flag $(V_i)_{i=1}^\ell$ associated to v lies in $Y_\beta \subset X_\alpha$, and this flag is a complete invariant of the P_α -orbit of v : one has $P_\alpha v = P_\alpha v'$ if and only if $V_i = V'_i$ for $i = 1, 2, \dots, \ell$. This gives a bijection $P_\alpha \backslash \mathbb{F}_{q^m}^n \rightarrow X_\alpha$. \square

Something even more striking is true, regarding the action of the cyclic group $C = \mathbb{F}_{q^m}^\times$ on the set of flags X_α inside \mathbb{F}_{q^m} . Fix a multiplicative generator γ for $C = \langle \gamma \rangle = \mathbb{F}_{q^m}^\times$, so γ has multiplicative order $q^m - 1$. Also fix a primitive $(q^m - 1)$ st root of unity ζ in \mathbb{C}^\times . For an element γ^d in C , denote its fixed subset by

$$(X_\alpha)^{\gamma^d} := \{x \in X_\alpha : \gamma^d(x) = x\}.$$

Proposition 6.14. *For any composition α and integer d , one has*

$$|(X_\alpha)^{\gamma^d}| = [C_{\alpha,m}(t)]_{t=\zeta^d}.$$

In other words, the triple $(X_\alpha, C_{\alpha,m}(t), C)$ exhibits a cyclic sieving phenomenon in the sense of [19].

Proof. It follows from [19, Theorem 9.4] that for a weak composition β with $|\beta| \leq m$ and integer d , one has

$$|(Y_\beta)^{\gamma^d}| = \left[\begin{matrix} m \\ \beta, m - |\beta| \end{matrix} \right]_{q,t=\zeta^d}.$$

So by (1.6) suffices to show $(Y_\beta)^{\gamma^d} \neq \emptyset$ implies that $[t^{e(m,\alpha,\beta)}]_{t=\zeta^d} = 1$.

One checks this as follows. Let r be the multiplicative order of γ^d within $C = \mathbb{F}_{q^m}^\times$, and of ζ^d within \mathbb{C}^\times . One knows that $\mathbb{F}_q(\gamma^d) = \mathbb{F}_{q^\ell}$ for some divisor ℓ of m with the property that r divides $q^\ell - 1$. Then any $(\beta, m - |\beta|)$ -flag of \mathbb{F}_q -subspaces in \mathbb{F}_{q^m} stabilized by γ^d must actually be a flag of $\mathbb{F}_q(\gamma^d)$ -subspaces, and hence a flag of \mathbb{F}_{q^ℓ} -subspaces. Therefore ℓ must divide each partial sum B_i for $i = 1, 2, \dots, \ell$. As ℓ also divides m , this means that ℓ divides each $m - B_i$, so that $q^\ell - 1$ divides each $q^{m-B_i} - 1$, and hence $q^\ell - 1$ divides each $q^m - q^{B_i} = q^{B_i}(q^{m-B_i} - 1)$. This means that r will also divide each $q^m - q^{B_i}$, so that r divides $e(m, \alpha, \beta)$, and $[t^{e(m, \alpha, \beta)}]_{t=\zeta^d} = 1$ as desired. \square

One can reinterpret Proposition 6.14 in the following fashion.

Proposition 6.14'. *Parabolic Conjecture 1.1 implies that for any field $k \supset \mathbb{F}_{q^m}$, one has a kC -module isomorphism of the P_α -fixed spaces*

$$(6.4) \quad Q_k^{P_\alpha} \cong k[\mathbb{F}_{q^m}^n]^{P_\alpha}.$$

Proof. Note that $|C| = q^m - 1$ is relatively prime to the characteristic of $k \supset \mathbb{F}_q$, and hence kC is semisimple. Thus it suffices to check that $Q_k^{P_\alpha}$ and $k[\mathbb{F}_{q^m}^n]^{P_\alpha}$ have the same kC -module Brauer characters. Recall [22, §18.1] that to compute these Brauer characters, one starts by fixing an embedding of cyclic groups

$$\begin{aligned} C = \mathbb{F}_{q^m}^\times = \langle \gamma \rangle &\longrightarrow \mathbb{C}^\times \\ \gamma^d &\longmapsto \zeta^d \quad \text{where } \zeta := e^{\frac{2\pi i}{q^m-1}}. \end{aligned}$$

Then whenever an element γ^d in C acts in some r -dimensional $\mathbb{F}_{q^m}C$ -module U with multiset of eigenvalues $(\gamma^{i_1}, \dots, \gamma^{i_r})$, its Brauer character value on U is defined to be

$$\chi_U(\gamma^d) := \zeta^{i_1} + \dots + \zeta^{i_r}.$$

To compute Brauer character values on $Q_k^{P_\alpha}$, recall from Definition 6.6 that the element γ^d in C acting on this graded vector space will scale the e th homogeneous component by $(\gamma^d)^e$. Hence

$$(6.5) \quad \chi_{Q_k^{P_\alpha}}(\gamma^d) = \left[\text{Hilb} \left(Q_k^{P_\alpha}, t \right) \right]_{t=\zeta^d}.$$

To compute the Brauer character values on $k[\mathbb{F}_{q^m}^n]^{P_\alpha}$, note that since $k[\mathbb{F}_{q^m}^n]$ is a permutation representation of $P_\alpha \times C$, its P_α -fixed space $k[\mathbb{F}_{q^m}^n]^{P_\alpha}$ is isomorphic to the permutation representation of C on the set of P_α -orbits on $P_\alpha \backslash \mathbb{F}_{q^m}^n$. Equivalently, by Theorem 6.13, this is the permutation representation of C on X_α . For a *permutation* representation of a finite group, it is easily seen that its Brauer character value for a (p -regular) element is its usual ordinary complex character value, that is, its number of fixed points. Hence the Brauer character value for γ^d when acting on $k[\mathbb{F}_{q^m}^n]^{P_\alpha}$ is $|(X_\alpha)^{\gamma^d}|$. Comparing this value with (6.5), and assuming Parabolic Conjecture 1.1, one finds that Proposition 6.14 exactly asserts that the two kC -modules in (6.4) have the same Brauer characters. \square

7. FURTHER QUESTIONS AND REMARKS

7.1. The two limits where t, q go to 1. In [18, (1.3)], it was noted that two different kinds of limits applied to the (q, t) -binomials yield the same answer after swapping q and t , namely

$$\lim_{t \rightarrow 1} \begin{bmatrix} n \\ k \end{bmatrix}_{q,t} = \begin{bmatrix} n \\ k \end{bmatrix}_q \quad \text{and} \quad \lim_{q \rightarrow 1} \begin{bmatrix} n \\ k \end{bmatrix}_{q,t} = \begin{bmatrix} n \\ k \end{bmatrix}_t.$$

One can similarly apply these two kinds of limits to $C_{n,m}(t)$, giving two somewhat different answers:

$$(7.1) \quad \lim_{t \rightarrow 1} C_{n,m}(t) = \sum_{k=0}^{\min(n,m)} \begin{bmatrix} m \\ k \end{bmatrix}_q$$

$$(7.2) \quad \lim_{q \rightarrow 1} C_{n,m}(t^{\frac{1}{q-1}}) = \sum_{k=0}^{\min(n,m)} t^{(n-k)(m-k)} \begin{bmatrix} m \\ k \end{bmatrix}_t.$$

The limit (7.1) can be interpreted, via Theorem 6.13 for $\alpha = (n)$, as counting $GL_n(\mathbb{F}_q)$ -orbits on $\mathbb{F}_{q^m}^n$. When $m \geq n$, it gives the *Galois number* G_n counting all \mathbb{F}_q -subspaces of \mathbb{F}_q^n and studied, e.g., by Goldman and Rota [9]. We have no insightful explanation or interpretation for the limit (7.2).

In addition, it is perhaps worth noting two further specializations of (7.2): setting $m = n$ or $m = n - 1$, and then taking the limit as $n \rightarrow \infty$, one obtains the left sides of the two *Rogers-Ramanujan identities*:

$$\sum_{k=0}^{\infty} \frac{t^{k^2}}{(t; t)_k} = \frac{1}{(t; t^5)_{\infty} (t^4; t^5)_{\infty}} \quad \text{and} \quad \sum_{k=0}^{\infty} \frac{t^{k^2+k}}{(t; t)_k} = \frac{1}{(t^2; t^5)_{\infty} (t^3; t^5)_{\infty}}$$

where $(x; t)_k := (1 - x)(1 - tx) \cdots (1 - t^{k-1}x)$ and $(x; t)_{\infty} = \lim_{k \rightarrow \infty} (x; t)_k$. We have no explanation for this.

7.2. G -fixed divided powers versus G -cofixed polynomials. We reformulate Conjecture 1.2 slightly.

Setting $V := \mathbb{F}_q^n$, one can regard the symmetric algebra $S = \mathbb{F}_q[x_1, \dots, x_n] = \text{Sym}(V^*)$ as a *Hopf algebra*, which is graded of *finite type*, meaning that each graded piece S_d is finite-dimensional. Then the (restricted) dual Hopf algebra $D(V)$ has as its d th graded piece $D(V)_d = S_d^*$, the \mathbb{F}_q -dual vector space to S_d , and naturally carries the structure of a *divided power algebra* on V ; see, e.g., [1, §I.3, I.4]. Consequently, Proposition 3.3 implies that the G -fixed space $D(V)_d^G$ is \mathbb{F}_q -dual to the G -cofixed space $(S_d)_G$, so that

$$\text{Hilb}(D(V)^G, t) = \text{Hilb}(S_G, t).$$

This means one can regard Conjecture 1.2 as being about $\text{Hilb}(D(V)^G, t)$ instead. Since $D(V)^G$ is a subalgebra of the divided power algebra $D(V)$, this suggests the following.

Question 7.1. For $V = \mathbb{F}_q^n$ and $G = GL_n(\mathbb{F}_q)$, is Conjecture 1.2 suggesting a predictable or well-behaved ring structure for the G -fixed subalgebra $D(V)^G$ of the divided power algebra $D(V)$?

The invariant theory literature for finite subgroups of $GL(V)$ acting on divided powers $D(V)$ is much less extensive than the literature for actions on polynomial rings $S = \text{Sym}(V)$, although one finds a few results in Segal [21]. M. Crabb² informs us that, in work with J. Hubbuck and a student D. Salisbury, some results on the structure of $D(V)^G$ were known to them for $G = GL_2(\mathbb{F}_p)$ acting on $V = \mathbb{F}_p^2$ with $p = 2, 3$.

7.3. Approaches to Conjecture 1.1. In approaching Conjecture 1.1 we would like an explicit \mathbb{F}_q -basis for Q^G where $Q = S/\mathfrak{m}^{[q^m]}$, in degrees suggested by the (q, t) -binomial summands in the formula (1.2) for $C_{n,m}(t)$. For example, when $m \geq n$ one can at least make a reasonable guess about *part* of such a basis that models the $k = n$ summand in (1.2), as follows. It was shown in [18, (5.6)] that

$$\begin{bmatrix} m \\ n \end{bmatrix}_{q,t} = \sum_{(\lambda, a)} t^{\sum_{i=0}^{n-1} a_i (q^n - q^{n-i})}$$

where (λ, a) ranges over all pairs in which $\lambda = (\lambda_1, \dots, \lambda_n)$ satisfies $m - n \geq \lambda_1 \geq \dots \geq \lambda_n \geq 0$, and $a = (a_0, \dots, a_{n-1})$ is a tuple of nonnegative integers q -compatible with λ in the sense that $a_i \in [\delta_i, \delta_i + q^{\lambda_i}]$, where $\delta_i := q^{\lambda_{i+1}} + q^{\lambda_{i+1}+1} + \dots + q^{\lambda_i-1}$. Thus one might guess that the images of the monomials $\prod_{i=0}^{n-1} D_{n,n-i}^{a_i}$ as one ranges over the same pairs of (λ, a) form part of an \mathbb{F}_q -basis for Q^G , and their \mathbb{F}_q -linear independence has been checked computationally for a few small values of n, m, q .

However, one knows that at least *some* of the basis elements accounting for other summands in (1.2) are *not* sums of products of Dickson polynomials $D_{n,i}$, as the natural map $S^G \rightarrow Q^G$ is *not* surjective for $n \geq 2$. One seems to need recursive constructions, that produce invariants in n variables from invariants in $n - 1$ variables, with predictable effects on the degrees. Currently, we lack such constructions.

Non-surjectivity of $S^G \rightarrow Q^G$ appears in another initially promising approach. As $\mathfrak{m}^{[q^m]} = (x_1^{q^m}, \dots, x_n^{q^m})$ is generated by a regular sequence on S , one has an S -free *Koszul resolution* [16, §XVI.10] for $Q = S/\mathfrak{m}^{[q^m]}$:

$$0 \rightarrow S \otimes_{\mathbb{F}} \wedge^n V \rightarrow \dots \rightarrow S \otimes_{\mathbb{F}} \wedge^2 V \rightarrow S \otimes_{\mathbb{F}} \wedge^1 V \rightarrow S \rightarrow Q \rightarrow 0.$$

Taking G -fixed spaces gives a *complex*, which is generally not exact when $\mathbb{F}_q G$ is not semisimple, but at least contains Q^G at its right end:

$$(7.3) \quad 0 \rightarrow (S \otimes_{\mathbb{F}} \wedge^n V)^G \rightarrow \dots \rightarrow (S \otimes_{\mathbb{F}} \wedge^2 V)^G \rightarrow (S \otimes_{\mathbb{F}} \wedge^1 V)^G \rightarrow S^G \rightarrow Q^G \rightarrow 0.$$

A result of Hartmann and Shepler [10, §6.2] very precisely describes each term $(S \otimes_{\mathbb{F}} \wedge^i V)^G$ in (7.3) as a free S^G -module with explicit S^G -basis elements that are homogeneous with predictable degrees; this is an analogue of a classic result on invariant differential forms for complex reflection groups due to Solomon [24]. Thus each term $(S \otimes_{\mathbb{F}} \wedge^i V)^G$ has a simple explicit Hilbert series. However, non-exactness means that (7.3) is not a resolution of Q^G , so it does not let us directly compute its Hilbert series.

²Personal communication, 2013.

7.4. Rational Cherednik algebras for $GL_n(\mathbb{F}_q)$. Section 6 alluded to the considerations that led to Conjecture 1.1, coming from the theory of real reflection groups W . When W acts irreducibly on \mathbb{R}^n and on the polynomial algebra $\mathbb{C}[\mathbf{x}] = \mathbb{C}[x_1, \dots, x_n]$, one can define its graded W -parking space $\mathbb{C}[\mathbf{x}]/(\theta_1, \dots, \theta_n)$, as a quotient by a certain homogeneous system of parameters $\theta_1, \dots, \theta_n$ of degree $h+1$ inside $\mathbb{C}[\mathbf{x}]$, where h is the *Coxeter number* of W ; see [2].

Replacing W by $G := GL_n(\mathbb{F}_q)$, we think of $h := q^n - 1$ as the *Coxeter number*, with $x_i^{q^n}$ playing the role of θ_i , and $Q = S/\mathfrak{m}^{q^n}$ playing the role of the graded G -parking space.

In the real reflection group theory, the W -parking space carries the structure of an irreducible finite dimensional representation $L_c(\text{triv})$ for the *rational Cherednik algebra* $H_c(W)$ with parameter value $c = \frac{h+1}{h}$. Here the θ_i span the common kernel of the *Dunkl operators* in $H_c(W)$ when acting on $\mathbb{C}[\mathbf{x}] = M_c(\text{triv})$. In addition, its W -fixed space $L_c(\text{triv})^W$ is a graded subspace whose Hilbert series is the *W-Catalan polynomial*.

This explains why we examined the Hilbert series of Q^G in our context. In fact, rational Cherednik algebras $H_c(G)$ for $G = GL_n(\mathbb{F}_q)$ and their finite dimensional representations $L_c(\text{triv})$ have been studied by Balagović and Chen [4]. However, their results show that the common kernel of the Dunkl operators in $H_c(G)$ acting on $S = \mathbb{F}_q[\mathbf{x}]$ is *not* spanned by $x_1^{q^n}, \dots, x_n^{q^n}$. In fact, for almost all choices of n and the prime power $q = p^r$, they show [4, Theorem 4.10] that it is spanned by x_1^p, \dots, x_n^p , independent of the exponent r .

Can one modify this rational Cherednik theory for G to better fit our setting, and gain insight into Q^G ?

APPENDIX A. PROOF OF PROPOSITION 2.1

We recall here the statement to be proven.

Proposition 2.1. *For any $m \geq 0$ and any composition α of n , the power series*

$$\text{Hilb}(S^{P_\alpha}, t) = \prod_{i=1}^{\ell} \prod_{j=0}^{\alpha_i-1} \frac{1}{1 - t^{q^{A_i} - q^{A_{i-1}+j}}}$$

is congruent in $\mathbb{Z}[[t]]/(t^{q^m})$ to the polynomial

$$C_{\alpha,m}(t) = \sum_{\substack{\beta: \beta \leq \alpha \\ |\beta| \leq m}} t^{e(m, \alpha, \beta)} \left[\beta, m - |\beta| \right]_{q,t} \quad \text{where} \quad e(m, \alpha, \beta) = \sum_{i=1}^{\ell} (\alpha_i - \beta_i)(q^m - q^{B_i}).$$

Fix $m \geq 0$. Throughout this proof, “ \equiv ” denotes equivalence in $\mathbb{Z}[[t]]/(t^{q^m})$.

Given the composition $\alpha = (\alpha_1, \dots, \alpha_\ell)$, denote its i th partial sum by $A_i = \alpha_1 + \alpha_2 + \dots + \alpha_i$ as before. Adopting the convention that $A_0 := 0, A_{\ell+1} := +\infty$, define L to be the largest index in $0 \leq L \leq \ell$ for which $A_L \leq m$, so that $A_{L+1} > m$. Part of the relevance of the index L comes from the truncation to the first L factors in the product formula

$$(A.1) \quad \text{Hilb}(S^{P_\alpha}, t) = \prod_{i=1}^{\ell} \prod_{j=0}^{\alpha_i-1} \left(1 - t^{q^{A_i} - q^{A_{i-1}+j}} \right)^{-1} \equiv \prod_{i=1}^L \prod_{j=0}^{\alpha_i-1} \left(1 - t^{q^{A_i} - q^{A_{i-1}+j}} \right)^{-1},$$

where the last equivalence is justified as follows. As q is a prime power, one has $q \geq 2$. Thus for integers a, b, c , one has

$$(A.2) \quad a > b, c \quad \text{implies} \quad q^a - q^b - q^c \geq q^a - 2q^{a-1} = (q-2)q^{a-1} \geq 0.$$

In particular, $q^{A_i} - q^{A_{i-1}+j} \geq q^{A_{i-1}} \geq q^m$ for all $i \geq L+1$. Thus, all of the factors in (A.1) with $i > L$ are equivalent to 1 modulo (t^{q^m}) .

We will make frequent use of (A.2); for example, it helps prove the following lemma, which shows that most summands of $C_{\alpha,m}(t)$ in (1.6) vanish in $\mathbb{Z}[[t]]/(t^{q^m})$.

Lemma A.1. *Given m and α , with A_i and L defined as above, the weak compositions $\beta = (\beta_1, \dots, \beta_\ell)$ with $0 \leq \beta \leq \alpha$ and $|\beta| \leq m$ for which $e(m, \alpha, \beta) < q^m$ are exactly those of the following two forms:*

$$(i) \quad \text{either } \beta = \hat{\alpha} := \begin{cases} \alpha & \text{if } L = \ell, \\ (\alpha_1, \dots, \alpha_L, m - A_L, 0, \dots, 0) & \text{otherwise,} \end{cases}$$

(ii) or for $k = 1, 2, \dots, L$,

$$\beta = \widehat{\alpha}^{(k)} := \begin{cases} (\alpha_1, \dots, \alpha_{k-1}, \alpha_k - 1, \alpha_{k+1}, \dots, \alpha_\ell) & \text{if } L = \ell, \\ (\alpha_1, \dots, \alpha_{k-1}, \alpha_k - 1, \alpha_{k+1}, \dots, \alpha_L, m - A_L + 1, 0, \dots, 0) & \text{otherwise.} \end{cases}$$

In the former case, $e(m, \alpha, \beta) = 0$, and in the latter, $e(m, \alpha, \beta) = q^m - q^{A_k - 1}$.

Proof of Lemma A.1. Assume $\beta = (\beta_1, \dots, \beta_\ell)$ has $0 \leq \beta \leq \alpha$, with $|\beta| \leq m$, and that $e(m, \alpha, \beta) < q^m$. As before, let $B_i = \beta_1 + \beta_2 + \dots + \beta_i$ for $i = 0, 1, \dots, \ell + 1$, with conventions $B_0 := 0$ and $B_{\ell+1} := m$. By (A.2), the condition $e(m, \alpha, \beta) < q^m$ implies that at most one summand in $e(m, \alpha, \beta)$ may be nonzero, and if the i th summand $(\alpha_i - \beta_i)(q^m - q^{B_i})$ is nonzero then $\alpha_i - \beta_i = 1$. Choose j minimal so that $0 \leq j \leq \ell + 1$ and $B_j = m$. We consider two cases, depending on whether or not $e(m, \alpha, \beta) = 0$.

Case 1. $e(m, \alpha, \beta) = 0$. In this case all summands in $e(m, \alpha, \beta)$ are zero, so $\beta_i = \alpha_i$ for all $i < j$. If $j = \ell + 1$ then it follows immediately that $\beta = \alpha = \widehat{\alpha}$. Otherwise, $j \leq \ell$. Since $B_j = m$ but $A_i = B_i < m$ for $i < j$, we have $j = L$. Therefore $\beta = (\alpha_1, \dots, \alpha_L, m - A_L, 0, \dots, 0) = \widehat{\alpha}$ in this case.

Case 2. $e(m, \alpha, \beta) > 0$. In this case there is an index k such that $k < j$ and $\alpha_i - \beta_i = 1$, and for all other $i < j$ we have $\beta_i = \alpha_i$. If $j = \ell + 1$ then it follows immediately that $\beta = (\alpha_1, \dots, \alpha_{k-1}, \alpha_k - 1, \alpha_{k+1}, \dots, \alpha_\ell) = \widehat{\alpha}^{(k)}$. Otherwise, $j \leq \ell$. Since $B_j = m$ but $A_i \leq B_i + 1 \leq m$ for $i < j$, we have $j = L$. Therefore $\beta = (\alpha_1, \dots, \alpha_{k-1}, \alpha_k - 1, \alpha_{k+1}, \dots, \alpha_L, m - A_L + 1, 0, \dots, 0) = \widehat{\alpha}^{(k)}$ in this case. \square

Returning to the proof of Proposition 2.1, note that Lemma A.1 implies

$$(A.3) \quad C_{\alpha, m}(t) \equiv \left[\frac{m}{\widehat{\alpha}} \right]_{q, t} + \sum_{k=1}^L t^{q^m - q^{A_k - 1}} \left[\frac{m}{\widehat{\alpha}^{(k)}} \right]_{q, t}.$$

We next process the summands on the right. By definition, one has that

$$t^{q^m - q^{A_k - 1}} \left[\frac{m}{\widehat{\alpha}^{(k)}} \right]_{q, t} = t^{q^m - q^{A_k - 1}} \prod_{j=0}^{A_L - 1} (1 - t^{q^m - q^j}) / \prod_{i=1}^L \prod_{j=0}^{\widehat{\alpha}_i^{(k)} - 1} (1 - t^{q^{\widehat{A}_i^{(k)}} - q^{\widehat{A}_{i-1}^{(k)} + j}}),$$

where here $\widehat{A}_i^{(k)} := \widehat{\alpha}_1^{(k)} + \dots + \widehat{\alpha}_i^{(k)}$ as usual. We will attempt to simplify the fraction on the right side, working mod (t^{q^m}) . Note that in its numerator, only $t^{q^m - q^{A_k - 1}}$ survives, as (A.2) implies $(q^m - q^{A_k - 1}) + (q^m - q^j) \geq q^m$. Meanwhile in its denominator, only the factors indexed by $i = 1, 2, \dots, k$ survive multiplication by $t^{q^m - q^{A_k - 1}}$ when working mod (t^{q^m}) : since $\widehat{A}_i^{(k)} \geq A_k$ for $i \geq k + 1$, (A.2) implies $(q^m - q^{A_k - 1}) + (q^{\widehat{A}_i^{(k)}} - q^{\widehat{A}_{i-1}^{(k)} + j}) \geq q^m$. Thus one has

$$\begin{aligned} t^{q^m - q^{A_k - 1}} \left[\frac{m}{\widehat{\alpha}^{(k)}} \right]_{q, t} &\equiv t^{q^m - q^{A_k - 1}} \prod_{i=1}^k \prod_{j=0}^{\widehat{\alpha}_i^{(k)} - 1} \left(1 - t^{q^{\widehat{A}_i^{(k)}} - q^{\widehat{A}_{i-1}^{(k)} + j}} \right)^{-1} \\ &= \left(\prod_{i=1}^{k-1} \prod_{j=0}^{\alpha_i - 1} \left(1 - t^{q^{A_i} - q^{A_{i-1} + j}} \right)^{-1} \right) \cdot t^{q^m - q^{A_k - 1}} \prod_{j=0}^{\alpha_k - 2} \left(1 - t^{q^{A_k} - q^{A_{k-1} + j}} \right)^{-1}. \end{aligned}$$

Using (A.2), the last, unparenthesized factor is equivalent mod (t^{q^m}) to

$$t^{q^m - q^{A_k - 1}} + \sum_{j=0}^{\alpha_k - 2} t^{q^m - q^{A_{k-1} + j}} = \sum_{j=0}^{\alpha_k - 1} t^{q^m - q^{A_{k-1} + j}}.$$

Consequently, one has

$$(A.4) \quad t^{q^m - q^{A_k - 1}} \left[\frac{m}{\widehat{\alpha}^{(k)}} \right]_{q, t} \equiv \left(\sum_{j=0}^{\alpha_k - 1} t^{q^m - q^{A_{k-1} + j}} \right) / \prod_{i=1}^{k-1} \prod_{j=0}^{\alpha_i - 1} (1 - t^{q^{A_i} - q^{A_{i-1} + j}}).$$

Similarly one finds that

$$(A.5) \quad \left[\frac{m}{\widehat{\alpha}} \right]_{q, t} = \prod_{j=0}^{A_L - 1} (1 - t^{q^m - q^j}) / \prod_{i=1}^L \prod_{j=0}^{\alpha_i - 1} (1 - t^{q^{A_i} - q^{A_{i-1} + j}}).$$

The numerator on the right side of (A.5) can be rewritten mod (t^{q^m}) using (A.2) as

$$\prod_{j=0}^{A_L-1} (1 - t^{q^m - q^j}) \equiv 1 - \sum_{j=0}^{A_L-1} t^{q^m - q^j} = 1 - \sum_{k=1}^L \sum_{j=0}^{\alpha_k-1} t^{q^m - q^{A_{k-1}+j}}.$$

Comparing this with (A.1) shows that

$$\begin{aligned} (A.6) \quad \left[\begin{matrix} m \\ \hat{\alpha} \end{matrix} \right]_{q,t} &= \text{Hilb}(S^{P_\alpha}, t) - \sum_{k=1}^L \left(\sum_{j=0}^{\alpha_k-1} t^{q^m - q^{A_{k-1}+j}} \right) / \prod_{i=1}^L \prod_{j=0}^{\alpha_i-1} (1 - t^{q^{A_i} - q^{A_{i-1}+j}}) \\ &\equiv \text{Hilb}(S^{P_\alpha}, t) - \sum_{k=1}^L \left(\sum_{j=0}^{\alpha_k-1} t^{q^m - q^{A_{k-1}+j}} \right) / \prod_{i=1}^{k-1} \prod_{j=0}^{\alpha_i-1} (1 - t^{q^{A_i} - q^{A_{i-1}+j}}). \end{aligned}$$

The last equivalence mod (t^{q^m}) arises since if $i \geq k$ then $A_i \geq A_k$, so $(q^m - q^{A_{k-1}+j}) + (q^{A_i} - q^{A_{i-1}+j}) \geq q^m$ by (A.2). Finally, combining (A.3), (A.4), and (A.6) shows that $C_{\alpha,m}(t) \equiv \text{Hilb}(S^{P_\alpha}, t)$, as desired.

APPENDIX B. PROOFS IN THE BIVARIATE CASE

Our goal here is to prove Parabolic Conjectures 1.1 and 1.2 for $n = 2$. Their equivalence for $n = 2$ was shown in Corollary 3.6, so we only prove Parabolic Conjecture 1.2.

The group $G = GL_2(\mathbb{F}_q)$ has only two parabolic subgroups P_α , namely the whole group $G = P_{(2)}$ itself and the Borel subgroup $B = P_{(1,1)}$. We establish Parabolic Conjecture 1.2 for these subgroups below in Theorems B.15 and B.10, respectively.

We consider the chain of subgroups

$$(B.1) \quad 1 \subset \begin{matrix} T \\ \parallel \\ \left\{ \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} : a, d \in \mathbb{F}_q^\times \end{matrix} \right\} \subset \begin{matrix} B \\ \parallel \\ \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} : a, d \in \mathbb{F}_q^\times, b \in \mathbb{F}_q \end{matrix} \right\} \subset \begin{matrix} G \\ \parallel \\ \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : ad - bc \in \mathbb{F}_q^\times \end{matrix} \right\}$$

We first recall the known descriptions of the invariant subrings for each of these subgroups, and then prove some preliminary facts about their cofixed quotients. Using this, we complete the analysis first for the quotient S_B , and finally for the quotient S_G .

B.1. The invariant rings. Acting on $S = \mathbb{F}_q[x, y]$, the tower of subgroups (B.1) induces a tower of invariant subalgebras $S \supset S^T \supset S^B \supset S^G$, with the following explicit descriptions. Abbreviate $X := x^{q-1}, Y := y^{q-1}$, and recall from the introduction that for $n = 2$ the two Dickson polynomials $D_{2,0}, D_{2,1}$ are defined by

$$(B.2) \quad \prod_{(c_1, c_2) \in \mathbb{F}_q^2} (t + c_1 x + c_2 y) = t^{q^2} + D_{2,1} t^q + D_{2,0} t.$$

Proposition B.1. *For $S = \mathbb{F}_q[x, y]$ one has*

- (i) $S^T = \mathbb{F}_q[X, Y]$,
- (ii) $S^B = \mathbb{F}_q[X, D_{2,1}]$, and
- (iii) $S^G = \mathbb{F}_q[D_{2,0}, D_{2,1}]$,

with explicit formulas

$$\begin{aligned} D_{2,1} &= Y^q + XY^{q-1} + \dots + X^{q-1}Y + X^q, \\ D_{2,0} &= XY^q + X^2Y^{q-1} + \dots + X^qY = XD_{2,1} - X^{q+1}. \end{aligned}$$

Proof. Assertion (i) is straightforward. Assertion (ii) follows from the work of Mui [17] or Hewett [11]. Assertion (iii) is Dickson's Theorem [7] for $n = 2$. The last two equalities follow from Steinberg's expressions

$$\begin{aligned} (B.3) \quad D_{2,1} &= \left| \begin{matrix} x & y \\ x^{q^2} & y^{q^2} \end{matrix} \right| / \left| \begin{matrix} x & y \\ x^q & y^q \end{matrix} \right| = \frac{xy^{q^2} - x^{q^2}y}{xy^q - x^qy} = Y^q + XY^{q-1} + \dots + X^{q-1}Y + X^q \\ D_{2,0} &= \left| \begin{matrix} x^q & y^q \\ x^{q^2} & y^{q^2} \end{matrix} \right| / \left| \begin{matrix} x & y \\ x^q & y^q \end{matrix} \right| = \frac{x^q y^{q^2} - x^{q^2} y^q}{xy^q - x^qy} = XY^q + X^2Y^{q-1} + \dots + X^qY \end{aligned}$$

for the $D_{n,i}$ as quotients of determinants [25]. \square

B.2. The cofixed spaces. The tower of subgroups in (B.1) induces quotient maps $S \twoheadrightarrow S_T \twoheadrightarrow S_B \twoheadrightarrow S_G$. The quotient map $S \twoheadrightarrow S_T$ is easily understood.

Proposition B.2. *A monomial $x^i y^j$ in S survives in the T -cofixed space S_T if and only if $q-1$ divides both i and j , that is, if and only if $x^i y^j = X^{i'} Y^{j'}$ for some i', j' . Furthermore these monomials $\{X^{i'} Y^{j'}\}_{i', j' \geq 0}$ form an \mathbb{F}_q -basis for S_T .*

Proof. Proposition 5.1(iv) implies that S_T is the quotient of S by the \mathbb{F}_q -subspace spanned by all elements $t(x^i y^j) - x^i y^j$. A typical element t in T sends $x \mapsto c_1 x$ and $y \mapsto c_2 y$ for some c_1, c_2 in \mathbb{F}_q^\times . Therefore

$$t(x^i y^j) - x^i y^j = (c_1^i c_2^j - 1)x^i y^j.$$

If both i, j are divisible by $q-1$ then this will always be zero, and otherwise, there exist choices of c_1, c_2 for which it is a nonzero multiple of $x^i y^j$. \square

In understanding the quotients S_P, S_G , it helps to define two \mathbb{F}_q -linear functionals on S that descend to one or both of S_P, S_G . They are used in the proof of Corollary B.6 below to detect certain nonzero products.

Definition B.3. Define two \mathbb{F}_q -linear functionals $S \xrightarrow{\mu, \nu} \mathbb{F}_q$ by setting $\mu(x^i y^j) = \nu(x^i y^j) = 0$ unless $q-1$ divides both i, j , and setting

$$\mu(X^i Y^j) = \begin{cases} 1 & \text{if } i, j \geq 1, \\ 0 & \text{if } i = 0 \text{ or } j = 0 \end{cases}$$

and

$$\nu(X^i Y^j) = \begin{cases} 1 & \text{if } i = 0, \\ 0 & \text{if } i \geq 1. \end{cases}$$

In other words, μ applied to $f(x, y)$ sums the coefficients in f on monomials of the form $X^i Y^j$ that are not pure powers X^i or Y^j , while ν sums the coefficients on the pure Y -powers Y^j . It should be clear from their definitions and Proposition B.2 that both μ, ν descend to well-defined \mathbb{F}_q -linear functionals on S_T .

Proposition B.4. *One has the following:*

- (i) *The functional $S \xrightarrow{\nu} \mathbb{F}$ descends to a well-defined functional on S_B .*
- (ii) *The functional $S \xrightarrow{\mu} \mathbb{F}$ descends to a well-defined functional on both S_B and S_G .*

Proof. The Borel subgroup B is generated by the torus T together with a transvection

$$(B.4) \quad \begin{array}{ccc} x & \xrightarrow{u} & x \\ y & \xrightarrow{u} & x + y, \end{array}$$

while the full general linear group G is generated by B together with a transposition σ that swaps x, y . Hence by Proposition 5.1(iv), it suffices to check that for every monomial $x^i y^j$, both μ, ν vanish on

$$(B.5) \quad u(x^i y^j) - x^i y^j = \sum_{k=0}^{j-1} \binom{j}{k} x^{i+j-k} y^k$$

and that μ vanishes on

$$(B.6) \quad \sigma(x^i y^j) - x^i y^j = x^j y^i - x^i y^j.$$

The fact that μ vanishes on (B.6) is clear from the symmetry between X and Y in its definition.

To see that ν vanishes on (B.5), observe that ν vanishes on every monomial $x^{i+j-k} y^k$ appearing in the sum, as $k < j$ means it is never a pure power of y (or Y).

To see that μ vanishes on (B.5), we do a calculation. Applying μ to the right side gives

$$(B.7) \quad \sum_{k=0}^{j-1} \binom{j}{k} \mu(x^{i+j-k} y^k) = \sum_{\substack{k=1,2,\dots,j-1 \\ q-1 \text{ divides } k}} \binom{j}{k}$$

which equals the sum (in \mathbb{F}_q) of the coefficients on the monomials of the form $x^{\ell(q-1)}$ within the polynomial

$$f(x) := \sum_{k=1}^{j-1} \binom{j}{k} x^k = (x+1)^j - (x^j + 1).$$

One can then advantageously rewrite (B.7) by taking advantage of a root of unity fact:

$$\sum_{\beta \in \mathbb{F}_q^\times} \beta^k = \begin{cases} q-1 = -1 & \text{if } k = \ell(q-1) \text{ for some } \ell \in \mathbb{Z}, \\ 0 & \text{otherwise.} \end{cases}$$

Noting also that $f(0) = 0$, this lets one rewrite the right side of (B.7) as

$$\begin{aligned} - \sum_{\beta \in \mathbb{F}_q^\times} f(\beta) &= - \sum_{\beta \in \mathbb{F}_q} f(\beta) = - \sum_{\beta \in \mathbb{F}_q} (\beta+1)^j + \sum_{\beta \in \mathbb{F}_q} \beta^j + \sum_{\beta \in \mathbb{F}_q} 1 \\ &= - \sum_{\beta \in \mathbb{F}_q} \beta^j + \sum_{\beta \in \mathbb{F}_q} \beta^j + q = 0. \end{aligned} \quad \square$$

The following technical lemma on vanishing and equalities lies at the heart of our analysis of S_B , S_G .

Lemma B.5. *Beyond the vanishing in S_T of monomials except for $\{X^i Y^j\}_{i,j \geq 0}$, in the further quotient S_B one also has*

- (i) $X^i = 0$ for all $i \geq 1$,
- (ii) $X^i Y^j = X^{i'} Y^{j'}$ for all $i, i' \geq 1$ and $1 \leq j, j' \leq q$ if $i + j = i' + j'$.

In the even further quotient S_G , one additionally has

- (iii) $Y^j = 0$ for all $j \geq 1$, and
- (iv) $X^i Y^j = X^{i'} Y^{j'}$ for all $i, i', j, j' \geq 1$ with $i + j = i' + j' \leq 2q$.

Proof. For (i), since B contains the transvection u from (B.4), one has in S_B for any $k > 0$ that

$$0 \equiv u(x^{k-1}y) - x^{k-1}y = x^{k-1}(x+y) - x^{k-1}y = x^k.$$

Hence $X^i = x^{i(q-1)}$ vanishes in S_B for all $i > 0$.

For (ii), we claim that it suffices to show that whenever $i, j \geq 1$ and $2 \leq j \leq q$, one can express $X^i Y^j$ as a sum of $X^{i'} Y^{j'}$ having $i + j = i' + j'$ and $j' < j$: then all such monomials $X^i Y^j$ will be scalar multiples of each other, but they all take the same value 1 when one applies the functional μ from Definition B.3 and Proposition B.4, so they must all be equal.

To this end, let $d := (i+j)(q-1) = \deg(X^i Y^j)$. Using the transvection u from (B.4), and taking advantage of the vanishing of $x^i y^j$ in S_B unless $q-1$ divides i, j , one has

$$\begin{aligned} 0 &\equiv u(x^{d-(jq-1)} y^{jq-1}) - x^{d-(jq-1)} y^{jq-1} \\ &= x^{d-(jq-1)} (x+y)^{jq-1} - x^{d-(jq-1)} y^{jq-1} \\ &= \left(\sum_{k=0}^{jq-1} \binom{jq-1}{k} x^{d-k} y^k \right) - x^{d-(jq-1)} y^{jq-1} \\ &\equiv \binom{jq-1}{j(q-1)} x^{i(q-1)} y^{j(q-1)} + \sum_{m=0}^{j-1} \binom{jq-1}{m(q-1)} x^{(i+j-m)(q-1)} y^{m(q-1)} \\ &= \binom{jq-1}{j(q-1)} X^i Y^j + \sum_{m=0}^{j-1} \binom{jq-1}{m(q-1)} X^{i+j-m} Y^m. \end{aligned}$$

Thus it remains only to show that $\binom{jq-1}{j(q-1)} \neq 0$ in \mathbb{F}_q when $1 \leq j \leq q$. Letting $q = p^s$ for some prime p and exponent $s \geq 1$, we have

$$(B.8) \quad \binom{jq-1}{j(q-1)} = \frac{(jq-1)(jq-2) \cdots (jq-j+1)}{1 \cdot 2 \cdots (j-1)}.$$

For any integers a, b such that $1 \leq a \leq p^s - 1$ and $b \geq 1$, the largest power of p dividing $b \cdot p^s - a$ is equal to the largest power of p dividing a . Since $j \leq q$, it follows that the largest power of p dividing the numerator of the right side of (B.8) is equal to the largest power of p dividing the denominator, so $\binom{j^{q-1}}{j(q-1)} \neq 0$ in \mathbb{F}_q .

For (iii), note that since (i) implies X^i vanishes in S_B , the same vanishing holds in the further quotient S_G . But then Y^i also vanishes in S_G by applying the transposition σ in G swapping x, y .

For (iv), note that (ii) shows that, fixing $d := i + j$, all monomials $X^i Y^j$ with $i, j \geq 1$ and $j \leq q$ are equal in S_B , and hence also equal in the further quotient S_G . Applying the transposition σ as before, one concludes that these monomials are also all equal to the monomials $X^i Y^j$ with $i, j \geq 1$ and $i \leq q$. But when $d = i + j \leq 2q$ these two sets of monomials exhaust all of the possibilities for $X^i Y^j$ with $i, j \geq 1$. \square

The following corollary will turn out to be a crucial part of the structure of S_G as an S^G -module in the bivariate case, used in the proof of Theorem B.15 below. It is also consistent with the $n = 2$ case of Conjecture 5.9.

Corollary B.6. *In the G -fixed quotient space S_G , the images of the monomials*

$$(B.9) \quad \{1, XY, X^2Y, \dots, X^{q-2}Y\}$$

are all annihilated by $D_{2,0}$, but none of them is annihilated by any power of $D_{2,1}$.

Proof. Proposition B.1 shows that $D_{2,0}$ is a sum of q monomials of the form $X^i Y^j$ with $i, j \geq 1$. The same is true for the product $D_{2,0} \cdot M$ where M is any of the monomials in (B.9). Since these monomials M have degree at most $(q-1)^2$, the product $D_{2,0} \cdot M$ has degree at most $q^2 - 1 + (q-1)^2 = 2q(q-1)$, and hence all q of the monomials in the product are equal to the same monomial M' by Lemma B.5(iv). Therefore $D_{2,0}M \equiv qM' = 0$ in S_G , as desired.

Proposition B.1 shows that $D_{2,1} = Y^q + XY^{q-1} + \dots + X^{q-1}Y + X^q$, a sum of $q+1$ monomials. Hence for $j \geq 0$, the power $D_{2,1}^j$ is a sum of $(q+1)^j$ monomials, of the form

$$D_{2,1}^j = Y^{qj} + \left(\sum_{i,j \geq 1} c_{i,j} X^i Y^j \right) + X^{qj}$$

with $\sum_{i,j \geq 1} c_{i,j} = (q+1)^j - 2$. Thus the \mathbb{F}_q -linear functional μ from Definition B.3 and Proposition B.4 has

$$\mu(D_{2,1}^j \cdot 1) = \mu(D_{2,1}^j) = (q+1)^j - 2 = 1^j - 2 = -1 \neq 0,$$

while for any of the rest of the monomials $M = X^i Y$ with $i \geq 1$ in (B.9), it has

$$\mu(D_{2,1} \cdot M) = (q+1)^j = 1^j = 1 \neq 0.$$

Thus no power $D_{2,1}^j$ annihilates any of the monomials in (B.9) within S_G . \square

B.3. Analyzing the fixed quotient S_B for the Borel subgroup $B = P_{(1,1)}$. One can regard the polynomial algebra S with its B -action as a module for the group algebra $S^B[B]$ having coefficients in the B -invariant subalgebra $S^B = \mathbb{F}_q[D_{2,1}, X]$. We begin by describing the $S^B[B]$ -module structure on S , and thereby deduce the S^B -module structure on the B -cofixed space S_B . For this purpose, we borrow an idea from Karagueuzian and Symonds [12, §2.1].

Definition B.7. Let \widehat{S} be the \mathbb{F}_q -subspace of S spanned by the monomials $\{x^i y^j : 0 \leq j \leq q^2 - q\}$.

It is easily seen that \widehat{S} is stable under the action of B , and also under multiplication by x and so by its B -invariant power $X = x^{q-1}$, so that \widehat{S} becomes an $\mathbb{F}_q[X][B]$ -module. Thus the tensor product

$$\mathbb{F}_q[D_{2,1}] \otimes_{\mathbb{F}_q} \widehat{S}$$

is naturally a module for the ring

$$\mathbb{F}_q[D_{2,1}] \otimes_{\mathbb{F}_q} \mathbb{F}_q[X][B] \cong \mathbb{F}_q[D_{2,1}, X][B] = S^B[B]$$

via the tensor product action

$$(a \otimes c)(b \otimes d) = ab \otimes cd$$

for any elements

$$a, b \in \mathbb{F}_q[D_{2,1}], \quad c \in \mathbb{F}_q[X][B], \quad \text{and} \quad d \in \widehat{S}.$$

Proposition B.8 (cf. [12, Lemma 2.5]). *The multiplication map*

$$\begin{array}{ccc} \mathbb{F}_q[D_{2,1}] & \otimes_{\mathbb{F}_q} \widehat{S} & \longrightarrow S \\ f_1 & \otimes f_2 & \longmapsto f_1 f_2 \end{array}$$

induces an $S^B[B]$ -module isomorphism. Hence as a module over $S^B = \mathbb{F}_q[D_{2,1}, X]$, one has an isomorphism

$$\mathbb{F}_q[D_{2,1}] \otimes_{\mathbb{F}_q} \widehat{S}_B \cong S_B.$$

Proof. The multiplication map is easily seen to be a morphism of $S^B[B]$ -modules, so it remains only to check that it is an \mathbb{F}_q -vector space isomorphism. This follows by iterating a direct sum decomposition

$$(B.10) \quad D_{2,1}S_d \oplus \widehat{S}_{d+q^2-q} = S_{d+q^2-q}$$

justified for $d \geq 0$ as follows. The leftmost summand $D_{2,1}S_d$ in (B.10) has as \mathbb{F}_q -basis the set $\{D_{2,1}x^i y^j\}_{i+j=d}$. Since (B.3) shows that $D_{2,1} = y^{q^2-q} + x^{q-1}y^{q^2-2q+1} + \dots + x^{q^2-q}$, the leading monomials in y -degree for $D_{2,1}S_d$ are

$$\{x^i y^{j'} : i + j' = d + q^2 - q \text{ and } j' \geq q^2 - q\}.$$

Meanwhile the summand \widehat{S}_{d+q^2-q} has as \mathbb{F}_q -basis the complementary set of monomials

$$\{x^i y^j : i + j = d + q^2 - q \text{ and } j < q^2 - q\}$$

within the set of all monomials $\{x^i y^j : i + j = d + q^2 - q\}$ that form an \mathbb{F}_q -basis for S_{d+q^2-q} . \square

In analyzing S_B , it therefore suffices to analyze \widehat{S}_B .

Proposition B.9. *Within the quotient space \widehat{S}_B , one has the following.*

- (i) $X^i Y^j \equiv X^{i+j-1} Y$ for all $i \geq 1$ and $1 \leq j \leq q-1$.
- (ii) *There is an \mathbb{F}_q -basis*

$$(B.11) \quad \{Y, XY, X^2 Y, X^3 Y, \dots\} \cup \{1, Y^2, Y^3, \dots, Y^{q-1}\}.$$

- (iii) *There is an $\mathbb{F}_q[X]$ -module direct sum decomposition $\widehat{S}_B = M_1 \oplus M_2$, where*
 - $M_1 = \mathbb{F}_q[X] \cdot Y$ is a free $\mathbb{F}_q[X]$ -module on the basis $\{Y\}$, and
 - M_2 is the $\mathbb{F}_q[X]$ -submodule spanned by

$$(B.12) \quad \{1, Y^2 - XY, Y^3 - X^2 Y, \dots, Y^{q-1} - X^{q-2} Y\},$$

having $\mathbb{F}_q[X]$ -module structure isomorphic to a direct sum of copies of the quotient module $\mathbb{F}_q[X]/(X)$ with the elements of (B.12) as basis.

Proof. Assertion (i). This follows from Lemma B.5(ii).

Assertion (ii). We first argue that the monomials in (B.11) span \widehat{S}_B . By Definition B.7, one has that \widehat{S} is \mathbb{F}_q -spanned by $\{x^i y^j : i \geq 0 \text{ and } 0 \leq j < q^2 - q\}$. Since monomials other than those of the form $X^i Y^j$ vanish in S_T and thus in its further quotient S_B , one concludes that \widehat{S}_B is \mathbb{F}_q -spanned by

$$\{X^i Y^j : i \geq 0 \text{ and } 0 \leq j < q\}.$$

Lemma B.5(i) says X^i vanishes in S_B for $i \geq 1$, so one may discard these monomials and still have a spanning set. Also, assertion (i) of the present proposition shows that one may further discard monomials of the form $X^i Y^j$ with $i \geq 1$ and $j > 1$. Thus \widehat{S}_B is \mathbb{F}_q -spanned by

$$\{X^i Y\}_{i \geq 0} \cup \{Y^j\}_{0 \leq j \leq q-1},$$

which is the same set as in (B.11).

To see that these monomials are \mathbb{F}_q -linearly independent in \widehat{S}_B or S_B , this table shows that they are separated in each degree by the \mathbb{F}_q -linear functionals μ and ν on S_B from Definition B.3 and Proposition B.4:

degree	0	1	2	3	...	$q-1$	q	$q+1$	$q+2$...
monomial	1	Y	$XY \ Y^2$	$X^2 Y \ Y^3$...	$X^{q-2} Y \ Y^{q-1}$	$X^{q-1} Y$	$X^{q-2} Y$	$X^{q-3} Y$...
μ value	0	0	1 0	1 0	...	1 0	1	1	1	...
ν value	1	1	0 1	0 1	...	0 1	0	0	0	...

Assertion (iii). First note that since $\{Y, XY, X^2Y, X^3Y, \dots\}$ is a subset of an \mathbb{F}_q -basis for \widehat{S}_B , the submodule $M_1 = \mathbb{F}_q[X] \cdot Y$ indeed forms a free $\mathbb{F}_q[X]$ -module on the basis $\{Y\}$ inside of \widehat{S}_B . Since

$$\{1\} \cup \{Y^j\}_{2 \leq j \leq q-1}$$

extends $\{Y, XY, X^2Y, X^3Y, \dots\}$ to an \mathbb{F}_q -basis for \widehat{S}_B , so does the set (B.12)

$$\{1\} \cup \{Y^j - X^{j-1}Y\}_{2 \leq j \leq q-1}.$$

In particular, none of these elements vanish in \widehat{S}_B , and $\widehat{S}_B = M_1 + M_2$ where M_2 is the $\mathbb{F}_q[X]$ -span of (B.12). On the other hand, each element of (B.12) is annihilated on multiplication by X : this holds for the monomial 1 since X vanishes in S_B by Lemma B.5(i), and it holds for $Y^j - X^{j-1}Y$ with $2 \leq j \leq q-1$ since $XY^j \equiv X^jY$ in S_B by Lemma B.5(ii). Thus M_2 has (B.12) as an \mathbb{F}_q -basis, and its $\mathbb{F}_q[X]$ -module structure is that of a free $\mathbb{F}_q[X]/(X)$ -module on this same basis. This also shows that one has a *direct* sum $\widehat{S}_B = M_1 \oplus M_2$. \square

The following is immediate from Proposition B.8 and B.9.

Theorem B.10. *One has a direct sum decomposition $S_B = M'_1 \oplus M'_2$ as modules for $S^B = \mathbb{F}_q[D_{2,1}, X]$, where*

- M'_1 is a free $\mathbb{F}_q[D_{2,1}, X]$ -module on $\{Y\}$, and
- M'_2 is a direct sum of copies of the quotient S^B -module $\mathbb{F}_q[D_{2,1}, X]/(X)$ with basis listed in (B.12).

In particular, one has

$$\text{Hilb}(S_B, t) = \frac{t^{q-1}}{(1-t^{q-1})(1-t^{q^2-q})} + \frac{1+t^{2(q-1)}+t^{3(q-1)}+\dots+t^{(q-1)^2}}{1-t^{q^2-q}}$$

which equals the prediction from Parabolic Conjecture 1.2 for $\alpha = (1, 1)$, namely

$$\text{Hilb}(S_B, t) = 1 + \frac{t^{q-1}}{1-t^{q-1}} + \frac{t^{2(q-1)}}{1-t^{q-1}} + \frac{t^{q^2+q-2}}{(1-t^{q-1})(1-t^{q^2-q})},$$

with the four summands corresponding to $\beta = (0, 0), (0, 1), (1, 0), (1, 1)$, respectively.

B.4. Analyzing the fixed quotient S_G for the full group $G = GL_2(\mathbb{F}_q) = P_{(2)}$. One can again regard the polynomial algebra S with its G -action as a module for the group algebra $S^G[G]$ with coefficients in the G -invariant subalgebra $S^G = \mathbb{F}_q[D_{2,0}, D_{2,1}]$. Our strategy here in understanding S_G as an S^G -module differs from the previous section, as we do not have a G -stable subspace in S acted on freely by $D_{2,1}$ to play the role of the B -stable subspace $\widehat{S} \subset S$. Instead we will work with quotients by $D_{2,1}$.

Proposition B.11. *One has an S^G -module isomorphism $(S/(D_{2,1}))_G \cong S_G/D_{2,1}S_G$.*

Proof. Both are isomorphic to $S/(D_{2,1}S + \text{span}_{\mathbb{F}_q}\{g(f) - f\}_{g \in G, f \in S})$. \square

We wish to first analyze $(S/(D_{2,1}))_G$ as an S^G -module. For this it helps that we already understand $(S/(D_{2,1}))_B$ as an S^B -module, due to the following result.

Proposition B.12. *The composite map $\widehat{S} \hookrightarrow S \twoheadrightarrow S/(D_{2,1})$ is an isomorphism of $\mathbb{F}_q[X][B]$ -modules, which then induces an isomorphism of $\mathbb{F}_q[X]$ -modules $\widehat{S}_B \cong (S/(D_{2,1}))_B$.*

Proof. The first assertion comes from Proposition B.8, and the second assertion follows from the first. \square

Proposition B.13. *The set*

$$(B.13) \quad \{1, XY, X^2Y, \dots, X^{q-2}Y\} \cup \{X^qY\}$$

generates $S_G/D_{2,1}S_G$ as a module over $\mathbb{F}_q[D_{2,0}]$, and hence generates S_G as module over $\mathbb{F}_q[D_{2,0}, D_{2,1}] = S^G$.

Proof. The second assertion follows from the first via this well-known general lemma.

Lemma B.14. *Let R be an \mathbb{N} -graded ring. Let $I \subset R_+ := \bigoplus_{d>0} R_d$ be a homogeneous ideal of positive degree elements. Let M be a \mathbb{Z} -graded R -module with nonzero degrees bounded below.*

Then a subset generates M as an R -module if and only if its images generate M/IM as R/I -module.

Proof of lemma. The “only if” direction is clear. For the “if” direction, one assumes that $\{m_i\}$ in M have $\{m_i + IM\}$ generating M/IM as R/I -module, and shows that every homogeneous element m in M lies in $\sum_i Rm_i$ via a straightforward induction on the degree of m . \square

Returning to the proof of the first assertion in the proposition, we use Proposition B.11 to work with $(S/(D_{2,1}))_G$ rather than $S_G/D_{2,1}S_G$. As noted in Proposition B.1, $D_{2,0} = XD_{2,1} - X^{q+1}$, and hence

$$D_{2,0} \equiv -X^{q+1} \pmod{(D_{2,1})}.$$

Thus via the quotient map $(S/(D_{2,1}))_B \rightarrow (S/(D_{2,1}))_G$, one obtains an $\mathbb{F}_q[D_{2,0}]$ -spanning set for $(S/(D_{2,1}))_G$ from any $\mathbb{F}_q[X^{q+1}]$ -spanning set of $(S/(D_{2,1}))_B$, or equivalently via Proposition B.12, from any $\mathbb{F}_q[X^{q+1}]$ -spanning set of \widehat{S}_B . Since \widehat{S}_B has as \mathbb{F}_q -basis the monomials $\{X^i Y\}_{i \geq 0} \cup \{1, Y^2, Y^3, \dots, Y^{q-1}\}$ from (B.11), it has as an $\mathbb{F}_q[X^{q+1}]$ -spanning set

$$\{X^i Y\}_{0 \leq i \leq q} \cup \{1, Y^2, Y^3, \dots, Y^{q-1}\}.$$

Thus, this set is an $\mathbb{F}_q[D_{2,0}]$ -spanning set for $(S/(D_{2,1}))_G$. However, Lemma B.5(iii) says that the pure powers $\{Y^j\}_{j \geq 1}$ all vanish in S_G , so one obtains this smaller $\mathbb{F}_q[D_{2,0}]$ -spanning set for $(S/(D_{2,1}))_G$:

$$\{1, XY, X^2 Y, \dots, X^{q-2} Y, X^{q-1} Y, X^q Y\}.$$

We claim that the second-to-last element $X^{q-1} Y$ on this list is also redundant, as it vanishes in $(S/(D_{2,1}))_G$. To see this claim, note that in $(S/(D_{2,1}))_G$ one has

$$0 \equiv D_{2,1} = Y^q + (XY^{q-1} + X^2 Y^{q-2} + \dots + X^{q-2} Y^2 + X^{q-1} Y) + X^q.$$

Here the two pure powers X^q, Y^q vanish in S_G and also in $(S/(D_{2,1}))_G$ due to Lemma B.5(i),(iii). Similarly, the $q-1$ monomials inside the parenthesis $X^i Y^{q-i}$ for $i = 1, 2, \dots, q-1$ are all equal to $X^{q-1} Y$ due to Lemma B.5(i). This implies $0 \equiv (q-1)X^{q-1} Y = -X^{q-1} Y$ as claimed. \square

Theorem B.15. *One has an S^G -module direct sum decomposition $S_G = N_1 \oplus N_2$, in which*

- $N_1 = S^G \cdot X^q Y$ is a free S^G -module on the basis $\{X^q Y\}$, and
- N_2 is the S^G -submodule spanned by the elements of (B.9), whose S^G -module structure is a direct sum of $q-1$ copies of $S^G/(D_{2,0})$ with the elements of (B.9) as basis.

In particular, in the bivariate case $n = 2$, Conjecture 5.9 holds, and one has

$$\begin{aligned} \text{Hilb}(S_G, t) &= \frac{t^{q^2-1}}{(1-t^{q^2-1})(1-t^{q^2-q})} + \frac{1+t^{2(q-1)}+t^{3(q-1)}+\dots+t^{(q-1)^2}}{1-t^{q^2-q}} \\ &= 1 + \frac{t^{2(q-1)}}{1-t^{q-1}} + \frac{t^{2(q^2-1)}}{(1-t^{q^2-1})(1-t^{q^2-q})}, \end{aligned}$$

so that Conjecture 1.2 holds.

Proof. Define N_1, N_2 to be the S^G submodules of S_G spanned by $\{X^q Y\}$ and of the elements of (B.9), respectively. Then Proposition B.13 implies $S^G = N_1 + N_2$. Note that Corollary B.6 already shows that the submodule N_2 has the claimed structure. In particular, $D_{2,0} \cdot N_2 = 0$, that is, $N_2 \subset \text{Ann}_{S_G} D_{2,0}$.

We claim that this forces $N_2 = S^G \cdot X^q Y \cong S^G$, that is, no element f in S^G can annihilate $X^q Y$. Otherwise, there would be an element $D_{2,0} f$ in S^G annihilating both N_1, N_2 , and hence annihilating all of S_G , contradicting the assertion from Proposition 5.7 that S_G is a rank one S^G -module.

Once one knows $N_2 = S^G \cdot X^q Y \cong S^G$, one can also conclude that the sum $S_G = N_1 + N_2$ is direct, since

$$N_1 \cap N_2 \subset \text{Ann}_{S_G}(D_{2,0}) \cap N_2 = 0. \quad \square$$

Remark B.16. Our proof for Parabolic Conjectures 1.1 and 1.2 with $n = 2$ is hands-on and technical. One might hope to use more of the results of Karagueuzian and Symonds [12, 13, 14]. They give a good deal of information about the action of $G = GL_n(\mathbb{F}_q)$ on $S = \mathbb{F}_q[x_1, \dots, x_n]$, by analyzing in some detail the structure of S as an $\mathbb{F}_q U$ -module, where U is the p -Sylow subgroup of G consisting of all unipotent upper-triangular matrices. We have not seen how to apply this toward resolving our conjectures in general.

REFERENCES

- [1] K. Akin, D.A. Buchsbaum, and J. Weyman, Schur functors and Schur complexes. *Adv. in Math.* **44** (1982), 207–278.
- [2] D. Armstrong, V. Reiner and B. Rhoades, Parking spaces, [arXiv:1204.1760](#).
- [3] M.F. Atiyah and I.G. Macdonald, Introduction to commutative algebra. Addison-Wesley Publishing Co., 1969.
- [4] M. Balagović and H. Chen, Representations of rational Cherednik algebras in positive characteristic. *J. Pure Appl. Algebra* **217** (2013), 716–740.
- [5] D.J. Benson, Polynomial invariants of finite groups. *London Mathematical Society Lecture Note Series* **190**. Cambridge University Press, Cambridge, 1993.
- [6] D. Bourguiba and S. Zarati, Depth and the Steenrod algebra. With an appendix by J. Lannes. *Invent. Math.* **128** (1997), 589–602.
- [7] L.E. Dickson, A fundamental system of invariants of the general modular linear group with a solution of the form problem. *Trans. Amer. Math. Soc.* **12** (1911), 75–98.
- [8] D.S. Dummit and R.M. Foote, Abstract algebra. Third edition. John Wiley & Sons, Inc., Hoboken, NJ, 2004.
- [9] J. Goldman and G.-C. Rota, The number of subspaces of a vector space. Recent Progress in Combinatorics (Proc. Third Waterloo Conf. on Combinatorics, 1968), pp. 75–83. Academic Press, New York, 1969.
- [10] J. Hartmann and A.V. Shepler, Reflection groups and differential forms. *Math. Res. Lett.* **14** (2007), 955–971.
- [11] T.J. Hewett, Modular invariant theory of parabolic subgroups of $GL_n(F_q)$ and the associated Steenrod modules. *Duke Math. J.* **82** (1996), 91–102.
- [12] D. Karagueuzian and P. Symonds, The module structure of a group action on a polynomial ring. *J. Algebra* **218** (1999), no. 2, 672–692.
- [13] D. Karagueuzian and P. Symonds, The module structure of a group action on a polynomial ring: examples, generalizations, and applications. Invariant theory in all characteristics, 139–158, *CRM Proc. Lecture Notes* **35**, Amer. Math. Soc., Providence, RI, 2004.
- [14] D. Karagueuzian and P. Symonds The module structure of a group action on a polynomial ring: a finiteness theorem. *J. Amer. Math. Soc.* **20**(2007), 931–967.
- [15] P. S. Landweber and R. E. Stong, The depth of rings of invariants over finite fields, *Springer Lect. Notes in Math.* **1240** (1987), 259–274.
- [16] S. Lang, Algebra. Revised third edition. *Graduate Texts in Mathematics* **211**. Springer-Verlag, New York, 2002.
- [17] H. Mui, Modular invariant theory and cohomology algebras of symmetric groups. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **22** (1975), no. 3, 319–369.
- [18] V. Reiner and D. Stanton, (q, t) -analogues and $GL_n(\mathbb{F}_q)$. *J. Algebraic Combin.* **31** (2010), 411–454.
- [19] V. Reiner, D. Stanton, and D. White, The cyclic sieving phenomenon. *J. Combin. Theory Ser. A* **108** (2004), 17–50.
- [20] B. Rhoades, Parking structures: Fuss analogs, [arXiv:1205.4293](#).
- [21] J. Segal, Notes on invariant rings of divided powers. Invariant theory in all characteristics, 229–239, *CRM Proc. Lecture Notes* **35**, Amer. Math. Soc., Providence, RI, 2004.
- [22] J.-P. Serre, Linear representations of finite groups. *Graduate Texts in Mathematics* **Vol. 42**. Springer-Verlag, New York-Heidelberg, 1977.
- [23] L. Smith, Polynomial invariants of finite groups. *Research Notes in Mathematics* **6**. A K Peters, Ltd., Wellesley, MA, 1995.
- [24] L. Solomon, Invariants of finite reflection groups. *Nagoya Math. J.* **22** (1963), 57–64.
- [25] R. Steinberg, On Dickson’s theorem on invariants. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **34** (1987), 699–707.

E-mail address: (jblewis,reiner,stanton)@math.umn.edu

SCHOOL OF MATHEMATICS, UNIVERSITY OF MINNESOTA, MINNEAPOLIS, MN 55455, USA